



用户使用指南





BitDefender 全方位安全杀毒软件

BitDefender 全方位安全杀毒软件

用户使用指南

出版方 2009.02.10

法律须知





目录











最终用户软件许可协议

如果您不赞同这些条款和条件，请不要安装此软件。无论在何种情况下，如果您点击"我接受"，"确定"，"继续"，"是" 或者安装、使用此软件，就表示您完全理解并接受本协议的所有条款。

产品注册。接受此协议表示您同意使用 “我的账户” 注册您的软件，作为您使用软件（接收升级）和获取支持的条件。这种控制帮助我们确保软件仅在合法授权的计算机上运行，获得合法授权的最终用户能够获得升级及支持服务。注册需要有效的产品序列号以及一个有效的电子邮件地址，以便接收更新及其他相关通知。

这些条款覆盖了BitDefender为家庭用户设计的解决方案和服务,包括相关的文档及购买许可证后进行的更新和升级,或在文档和这些条款的副本中规定的相关服务协议.

此使用许可协议是建立在您（个人或法人）和BitDefender之间的关于使用BitDefender软件产品的一份法律协议，以上所说的产品包括计算机软件以及相关多媒体产品，印刷资料，在线查阅的文档或者电子文档(“BitDefender”)，所有这些都受到国际版权法、国际版权条约的保护。只要您安装、拷贝或者使用BitDefender，就表示您愿意受到此协议条款的制约。

如果您不同意本协议的条款，请勿安装或使用BitDefender。

BitDefender 使用许可. BitDefender 是受版权法和国际版权条约及其它知识产权法律和条约所保护的。BitDefender 的使用权是一项特许授权，而不是一项买卖交易。

授权使用。BitDefender在此授予您并且仅授予您一人使用BitDefender的非专有权限。

应用软件。只要您有足够的授，您可以任意多计算机上安装并使用BitDefender。您可以制作一份额外拷贝用做备份用途。

桌面用户许可。该许可证能用于安装在某一不提供网络服务的电脑上的BitDefender软件。每一位初始用户都可以将这个软件安装在一台电脑上，并在另一台电脑上安装其副本。初始用户的数量等于许可证用户的数量。

授权条款。授权使用期限将从您安装、拷贝或者第一次使用BitDefender那天开始计算，并且将在授权码期限到期时失效。

过期。许可证一旦过期，此产品就立即停止运作。

升级。如果BitDefender被标记为升级版，则您必须被授权使用一个能被BITDEFENDER识别的产品来进行升级。被标记为升级版的BitDefender产品经替换或补充要被升级的产品。您只可在本授权协议条款下使用升级后的产品。如果BitDefender是您所购

买的一个软件包的某个组件的升级产品，则BitDefender可能会被用于软件包的一个组件升级，而不能被多于授权数量的其他用户单独使用。此协议中的条款将取代并覆盖在您和BITDEFENDER之间关于原产品及升级产品的任何之前协议。

版权。BitDefender的所有权益、称谓、利益，　以及BitDefender的所有版权（包括但不限于任何图象、照片、徽标、动画、视频、音频、音乐、文本以及小应用程序），　任何相关的印刷资料，以及所有的BitDefender的复制品都归BitDefender所有。BitDefender　受到版权法和国际条约的保护。因此您必须像对待其他受产权保护的物品一样对待BitDefender。您只可以在一台计算机上安装BitDefender，　并只能将原版用于备用或存档之用。您不能复印与BitDefender相关的印刷资料。无论以何种形式拷贝BitDefender，您都必须保留其原始形式的版权告示。您不可以自行再度授权、出租、出售，或租赁BitDefender。您不可以进行反向工程、重新编译、反汇编、创造衍生产品、修改、翻译、或进行任何获取BitDefender源代码的尝试。

有限质保。BitDefender保证从发货之日起的三十天之内，含有BitDefender的媒介不会出现质量问题。万一出现问题，BitDefender提供以下解决方案，您可以凭购买收据更换产品或者退款。BitDefender不保证BitDefender 将不被中断或者不发生错误或者错误将被改正。BitDefender不保证BitDefender 将符合您的要求。

除非在本协议中明文规定，BitDefender将不承担任何其他责任，无论明示或默认，BitDefender有权拒绝提供其他任何担保升级、维护或相关技术支持，或其他材料（有形的或无形的）及服务。无论用于法律法规、交易习惯、贸易惯例或业务习惯，BitDefender在此明确表示将无限制地放弃任何暗含保证和条件，包括拒绝提供任何可销售性或者符合某特定目的的暗含保证，如无干预、资料的准确性、信息内容的准确性、系统集成、通过过滤对第三方网站造成侵权或残缺、移除第三方网站的软件、间谍程序、广告软件、Cookie信息、电子邮件、文档、广告等。

不承诺损害赔偿。任何使用、测试、或评估BitDefender的人将自行承担所有对BitDefender 质量和性能造成的风险。BitDefender 在任何情况下都不对任何损害承担责任，包括任何情况下使用、性能或者交付BitDefender时带来的任何直接或间接的损害。

某些州不承认限制和排除事故或发生伤害的责任,所以以上限制可能不适用于您。

在任何情况下BITDEFENDER承担的责任不超过您的购买价格。该免责条款和限制将适用于无论您使用，评价，或测试BitDefender的情况。

对用户的重要告知。.　本软件并不具有容错性能，也不是为了在要求有自动防故障措施的危险环境中应用而专门设计的。本软件不适合应用于航空航天领域、核设施、或是通讯系统、武器系统、直接或间接的生命救护系统、空中交通管制系统、或是任何的由于系统失误可能导致死亡、严重身体伤害或者财产损害的任何应用领域或者设施。

同意电子通信。. BitDefender可能需要向您发送法律通知和其他有关软件及维护服务的信息（“通信”）。 BitDefender将通过产品内置的通知机制或用户注册时输入的电子邮件发送通信信息，或在其网站发布信息。如果接受本协议，您同意通过这些电子手段接收所有通信，并表明您可以使用通信网站。

常规。此协议受到罗马尼亚法律和国际版权规则和条约的管理。对于任何超出许可证条款而引发的纠纷，其专署管辖权和裁决权属于罗马尼亚法庭。

使用BitDefender的价格、花费和收费将随时变化，不会预先通知。

如果出现此协议有无效部分，无效的部分将不会影响此协议的其他部份的有效性。

BitDefender和BitDefender徽标是BitDefender的商标。所有其它商标都是其各自所有者的财产。

如果您违反了该许可证的条款和条件，此协议会在无任何通知的情况下立即终止。您无权因协议终止而要求BitDefender或任何BitDefender代理商处获得补偿。即便在协议终止后，有关保密及限制的条款依然有效。

BitDefender公司可以在任何时候修订这些条款，修订后的条款将自动应用于带有修订后条款的相应软件。如果在这些条款中有一部分是无效的和不可执行的，不会影响其他条款的有效性，它们仍然是有效的、可执行的。

由于将这些条款翻译成其他语言可能产生的争议或矛盾，BitDefender公司发行的英文版本是最权威的。

如欲联系BitDefender获得帮助或支持信息，请点击产品界面上的相关链接获得具体联系方式，或参考”关于“对话框中的详细信息。您也可发送邮件至如下地址: help@360.cn。



前言

本指南是专为引导选择BitDefender 全方位安全杀毒软件保安解决方案的用户而写的。本指南中的资料不仅适用于拥有电脑知识的人， 它同时适合任何能在视窗系统下工作的人。

这本书将给你介绍BitDefender 全方位安全杀毒软件安全系统的研发公司和团队,指导大家安装过程以及教导你如何设定系统。 你会学习到如何利用BitDefender 全方位安全杀毒软件如何更新、测试和设定。你也会学会如何从BitDefender取得最好的成效。

预祝您有个愉快而有益的阅读体验。

1. 本书中所使用的惯例

1.1. 字型

本书中使用了几种不同的字型,以提高本书的可读性。以下的表格将分别列出它们的意义。

显示	说明
`sample syntax`	格式示例采用 monospaced 字体显示。
http://www.bitdefender.com	链接到外部服务器的URL链接， 包括HTTP或FTP服务器。
support@bitdefender.com	电子邮件地址被插入文本内以提供联系信息
“前言” （第 xiv 页）	这是一个内部链接，指向本书内部的章节。
`filename`	文件和目录都使用 monospaced 字体。
option	所有产品选项都以粗体字显示。
`sample code listing`	代码采用monospaced字体显示。

1.2. 图标

图标是在附加在文内的说明，用图片标记，以方便您了解与当前段落有关的附加信息。



注意
注意事项的篇幅不长。虽然您可以忽视它，但它可能提供有用的信息，比如具体功能或指向其他相关主题的链接。



重要
需要您的注意，建议不要略过。 通常，它提供非关键但却重要信息。



警告
这是需要您更加认真阅读的关键信息。如果您遵照说明操作，就不会有任何不良后果。您应该阅读和理解其内容，因为其说明了一些非常危险的信息。

2. 本书的结构

这本书包括几个含有重要主题的部分。 此外，词汇表可以帮助您了解技术术语。

安装. BitDefender一步步的安装指示. 这是一个安装BitDefender 全方位安全杀毒软件的综合性的讲解。从安装成功的先决条件开始， 引导你经过整个安装进程。最后,这里也为你描述如何删除BitDefender。

基本管理. 描述BitDefender基本管理及维护功能

高级管理. BitDefender安全功能的详细介绍。 你学会了如何配置和使用所有的bitdefender模块等，以有效地保护您的计算机免受各种威胁（恶意软件，垃圾邮件，黑客， innapropriate内容等） 。

获得帮助. 出现意外状况时到何处求救

BitDefender救援光盘. BitDefender救援光盘的说明，有助于您理解和使用此可引导光盘的功能。

词汇表. 词汇表解释一些你会在此文档中遇到的不常见技术词汇。

3. 欢迎您的意见和建议

我们欢迎你对本书的改进提出意见，我们已经尽我们的所能验证所有的信息。如果你觉得这本书里有什么缺点，或认为有可以改善的地方，请写信给我们，以帮助我们提供更好的文档。

电子邮件可发送到 documentation@bitdefender.com.



重要
请用英语书写与文档相关的电子邮件，以便我们有效地处理。



安装

1. 系统需求

您可能会安装bitdefender全方位安全杀毒软件，只有在电脑上运行以下操作系统:

■Windows XP with Service Pack 2（32/64位）
■Windows Vista（32/64位）或 Windows Vista SP1
■Windows Home Server

在安装之前，请确保您的计算机满足最低的硬件和软件的要求。



注意
想了解您计算机上的Windows操作系统和硬件信息，请在我的电脑点击右键，然后从菜单中选择属性。

1.1. 硬件需求

Windows XP

■800MH或以上处理器
■256MB内存（推荐1GB）
■170MB可用硬盘空间（推荐200MB）

Windows Vista

■800MH或以上处理器
■512MB内存（推荐值1GB）
■170MB可用硬盘空间（推荐200MB）

Windows Home Server

■800MH或以上处理器
■512MB内存（推荐值1GB）
■170MB可用硬盘空间（推荐200MB）

1.2. 软件需求

■IE浏览器6.0或以上

■.NET Framework 1.1（包含在安装包中）

反钓鱼欺诈仅可用于下列软件:

■IE浏览器6.0或以上
■Mozilla Firefox 2.0
■雅虎通8.1
■MSN 8.5

即时通讯加密仅可用于下列软件:

■雅虎通8.1
■MSN 8.5

反垃圾邮件提供所有POP3/SMTP 电子邮件客户端的保护。 BitDefender反垃圾邮件的工具只集成到:

■Microsoft Outlook 2000, 2003, 2007
■Microsoft Outlook Express
■Microsoft Windows Mail
■Mozilla Thunderbird 1.5 and 2.0

2. 产品安装

双击安装程序，安装向导将会启动，并引导您进行整个安装过程。

在安装向导之前，Bitdefender将检查更新版本的安装包。如果发现有更新的版本，系统会提示您下载它。点击 是 可下载新的版本或否继续安装当前版本。



安装步骤



遵循这些步骤，以安装BitDefender全方位安全杀毒软件:

1. 点击 下一步 以继续或点击 取消 如果您想退出安装。
2. 点击 下一步。

   BitDefender 全方位安全杀毒软件能提示您的电脑上是否安装了其他杀毒软件. 点击 卸载 可以卸载该软件。 如果你想不卸载检测到的其他杀毒软件继续安装，请点击 下一步。



警告

安装BitDefender前，强烈建议您卸载其他杀毒软件。在一台电脑上同时运行两个或两个以上杀毒软件可能使系统瘫痪。

3. 请阅读用户使用协议并点击我同意。



重要

如果您不同意协议，请点击取消。 就会退出安装进程。

4. 你可以选择你想要安装本产品的文件夹。预设的文件夹是C:\Program Files\BitDefender\BitDefender 2009. 如果您想更改安装目录，请点击浏览并选择您要安装BitDefender的文件夹。

   点击 下一步。

5. 选择安装选项 有些选项是默认的:

   ■打开产品说明文档 - 在安装完成后打开产品说明文档。

   ■在桌面安装捷径 - 在安装完成后在桌面装置BitDefender全方位安全杀毒软件捷径

   ■安装完成后弹出光盘— 在安装完成后弹出光盘，这个选项在您通过光盘安装产品时会显示。

   ■关闭windows防火墙



重要

我们建议你关掉Windows防火墙自bitdefender全方位杀毒软件已包括一个先进的防火墙。运行两个防火墙，在同一部电脑上可能造成问题。

   ■关闭Windows Defender - 关闭Windows Defender，此选项只出现在Windows Vista上。

点击 安装 以开始安装产品。 如果之前未安装本产品，Bitdefender将首先安装.NET Framework 1.1。

请等待安装完成。

6. 点击完成。 安装向导会提示您重新启动你的系统，以便完成安装过程。 建议您尽快重新启动计算机。



重要

安装完成并重启计算机后，将会显示 注册向导 和 配置向导。 完成这些奇才队在以登记和配置Bitdefender全方位安全杀毒软件，并创造一种bitdefender帐户。

如果您选择了默认的安装路径，您将在Program Files文件夹下发现一个新的文件夹，名为BitDefender，它包含一个子文件夹 BitDefender 2009。

2.1. 注册向导

在安装完成后首次启动计算机时，将显示注册向导。 该向导可以帮助您激活Bitdefender并配置一个Bitdefender账户。

您必须创建一个BitDefender账户，以获得BitDefender更新。 该bitdefender账户还可让您获得免费的技术支持、特别优惠和促销产品。 如果您丢失了您的Bitdefender授权密钥，您可以登录到您的账户重新获取它，登录网址为http://myaccount.bitdefender.com。



注意

如果您不想进行此向导中的操作，请点击 取消。 您可随时进入注册向导，只需点击主界面底下的注册链接即可。

2.1.1. 步骤1/2- 注册 Bitdefender 全方位安全杀毒软件



注册

您可以看到Bitdefender注册状态，当前的授权密钥以及距离密钥过期所剩天数。

要继续试用产品，请选择继续使用当前密钥。

注册 Bitdefender 全方位安全杀毒软件

1. 选择我想要使用新的密钥注册产品。
2. 在编辑框中输入授权密钥。



注意

您可以找到您的授权密钥:

■在光盘标签上。

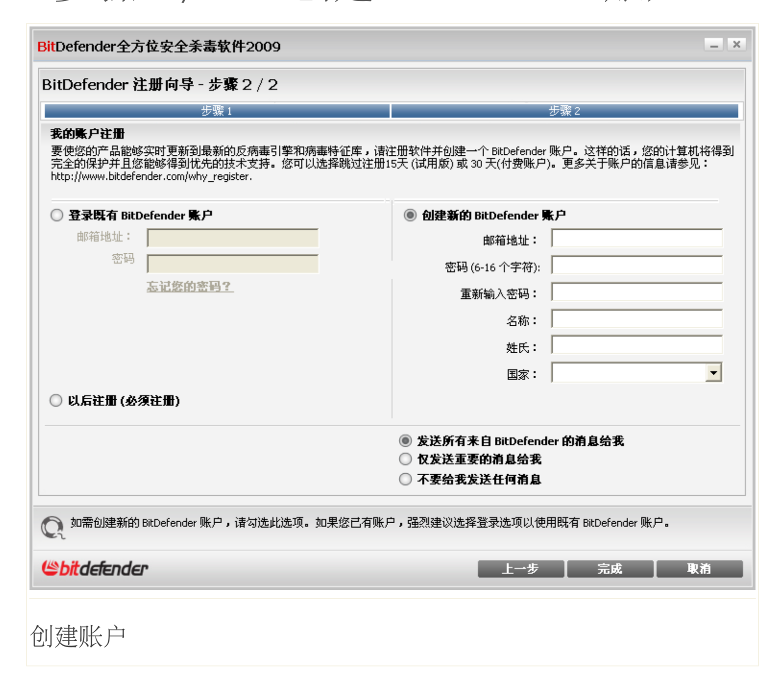
■在产品注册卡上。

■在网上购买的电子邮件中。

如果您没有Bitdefender授权密钥，请点击产品中所提供的链接前往Bitdefender网站购买。

点击 下一步 继续。

2.1.2. 步骤 2/2 – 创建BitDefender账户



创建账户

如果您此时不想创建Bitdefender账户，请选择跳过注册 并点击完成。 否则，根据您当前的情况继续进行：

- “我没有BitDefender账户” （第 9 页）
- “我已经有一个BitDefender账户” （第 9 页）



重要

您必须在安装BitDefender后15天内创建一个账户（如果您已注册产品，截止日期延长至30天）。 否则， BitDefender将不再更新。

我没有BitDefender账户

要创建BitDefender账户，请选择 新建Bitdefender账户并提供所需的信息。 您在这里提供的信息都将保密。

■电子邮件地址- 输入您的电子邮件地址。

■密码 – 输入您Bitdefender账户的密码。 密码不得少于6个字符。

■再次输入密码 – 请输入先前输入的密码。

■名字 – 您的名字。

■姓- 您的姓。

■国家 – 选择您居住的国家。



注意

使用您提供的电子邮件地址和密码登录您的账户：http://myaccount.bitdefender.com。

要成功建立账户，您必须先激活您的邮件地址。请检查您的邮件地址，并按照BitDefender注册服务系统发给您的邮件里的说明进行。

Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。 选择一个可用选项：

■请给我发送所有来自BitDefender的邮件
■仅发送重要消息
■不要给我发送任何消息

点击完成。

我已经有一个BitDefender账户

Bitdefender会自动检测你这台计算机以前是否注册过Bitdefender账户。 在这种情况下，请输入您账户的密码。

如果您已经有一个正常账户，但是Bitdefender没有检测到，请选择登录已存在的Bitdefender账户 并输入您账户的电子邮件地址和密码。

如果您忘记了密码，请点击忘记密码?然后按照说明进行。

Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。 选择一个可用选项:

■请给我发送所有来自BitDefender的邮件
■仅发送重要消息
■不要给我发送任何消息

点击完成。

2.2. 配置向导

在您完成注册向导后，配置向导将会出现。 该向导帮助您配置特定的产品模块并设置Bitdefender执行重要的安全任务。

完成向导进程并不是强制性的;但为了节约时间并保证系统在安装BitDefender全方位安全杀毒软件之前的安全性,我们推荐您完成该程序.



注意

如果您不想进行此向导中的操作，请点击 取消。 Bitdefender会在您打开用户界面时通知您需要配置的组件。

2.2.1. 步骤一 — 欢迎对话框



欢迎窗口

点击 下一步 继续。



2.2.2. 步骤 2/9 — 选择浏览模式



产品视图

请根据您使用BitDefender的经验选择两种用户界面之一:

■基本视图. 简单的用户界面，适合初学者和想要执行基本功能及快速解决问题的用户。 您只需注意Bitdefender的警告和警报，并修正出现的问题。

■高级视图. 高级界面，适合技术水平更高并希望能全面掌控产品的用户。 您可以设置产品的每个组件并执行高级任务。

点击 下一步 继续。

2.2.3. 步骤3/9: 配置bitdefender网络

BitDefender全方位安全杀毒软件2009

BitDefender 配置向导 - 步骤 3 / 9

步骤 1 | 步骤 2 | 步骤 3 | 步骤 4 | 步骤 5 | 步骤 6 | 步骤 7 | 步骤 8 | 步骤 9

家庭网络管理配置

BitDefender全方位安全杀毒软件2009 包含新的组件 - 家庭网络管理，这个功能允许您为您家庭中的所有计算机创建虚拟网络并管理所有安装于此网络的 BitDefender 产品。您将担任您创建的网络中的管理员或作为该网络中的成员接受其它计算机的管理。

如需作为 BitDefender 家庭网络中的成员，请勾选下方的复选框。您将被提示输入家庭管理密码以允许网络中的管理员远程控制此计算机的 BitDefender 设置及操作。

我想要作为 BitDefender 家庭网络中的成员

家庭管理密码：

重新输入密码：

如需获知关于 BitDefender 用户界面各选项的详情，请移动您的鼠标并悬停于相应窗口。此区域将显示相关的帮助文本。

bitdefender 上一步 下一步 取消

Bitdefender家庭网络配置

Bitdefender使您能够为您家里的计算机创建一个虚拟网络，从而可以管理安装在网络中计算机上的Bitdefender产品。

如果您希望此计算机成为Bitdefender家庭网络的一部分，请按照下列步骤进行:

1. 选择我想加入Bitdefender家庭网络。
2. 在各个编辑框中输入相同的管理密码。



重要

密码允许管理员在另外的计算机上管理本计算机上的Bitdefender产品。

点击 下一步 继续。

2.2.4. 步骤 4/9 –配置的身份控制

BitDefender全方位安全杀毒软件2009

BitDefender 配置向导 - 步骤 4 / 9

步骤 1 | 步骤 2 | 步骤 3 | 步骤 4 | 步骤 5 | 步骤 6 | 步骤 7 | 步骤 8 | 步骤 9

管理个人信息规则页面

BitDefender个人信息控制将帮助您保持您的私密数据安全并保护您不受敏感数据（如信用卡号码、邮箱地址等）窃取的侵害。

它也将通过扫描所有网络及邮件通信中的特定字串维护您数据的私密性。如需使用此特性，请启用并配置隐私控制模块。您在此输入的所有信息将被您的 Windows 账户证书加密。

☑ 我想要使用个人信息控制

添加 移除

规则名称	规则类型	HTTP	SMTP	即时...	关键词	区分大小写	描述
1	信用卡	是	是	否	是	否	

例外

bitdefender 上一步 下一步 取消

隐私控制设置

隐私控制保护您的敏感数据免受在线窃取。 基于您创建的规则，隐私控制扫描从您计算机发出的网页、电子邮件和即时通讯通信中是否包含特定字符串（例如，您的信用卡号码）。如果发现匹配，则对应的网页、电子邮件或即时讯息会被阻止。

如果您想要使用的隐私控制，请执行下列步骤:

1. 选择我想现在配置。
2. 创建规则以保护您的敏感数据。 欲了解更多信息，请参阅 “创建隐私控制规则” (第 15 页)。
3. 如果需要，请为您创建的规则定义特定的例外情况。 欲了解更多信息，请参阅 “定义隐私控制例外” (第 16 页)。

点击 下一步 继续。



创建隐私控制规则

要创建隐私规则，请点击添加。 配置窗口将会显示。



隐私控制规则

您必须设置以下参数:

■规则名称 – 请在此输入规则的名称。

■规则类型 – 选择规则类型（地址、姓名、信用卡、身份证等）。

■规则数据 – 请输入您希望保护的数据。 例如，如果您要保护您的信用卡号码，请在这里输入信用卡号码的全部或部分数字。



注意

如果您输入的字符少于三个，系统会提示您验证数据。我们推荐您输入至少三个字符，以避免误拦截网页或电子邮件。

您可以仅当规则全部匹配字符串或大小写匹配字符串时应用此规则。

为便于识别规则拦截的信息，请在此输入详细的规则描述。

如要指定扫描的通信类型，请设置这些选项:

■扫描HTTP – 扫描HTTP（网页）通信并阻止匹配上了规则的发出数据。

■扫描SMTP － 扫描SMTP（电子邮件）通信并阻止要发出的匹配上了规则的电子邮件。

■扫描即时通讯 － 扫描即时通讯流量并阻止要发出的包含规则数据的聊天信息。

点击 确定添加规则。

定义隐私控制例外

有时需要为特定的隐私规则定义例外条件。 例如，您定义了一个规则，以防止您的信用卡号码被通过HTTP（网页）发送出去。这样每当您在一个网站提交信用卡号码时，该网页都会被拦截。如果您想在购物网站上购物，您就必须为这个规则指定一个例外。

要打开管理例外的窗口，请点击例外。



隐私控制例外

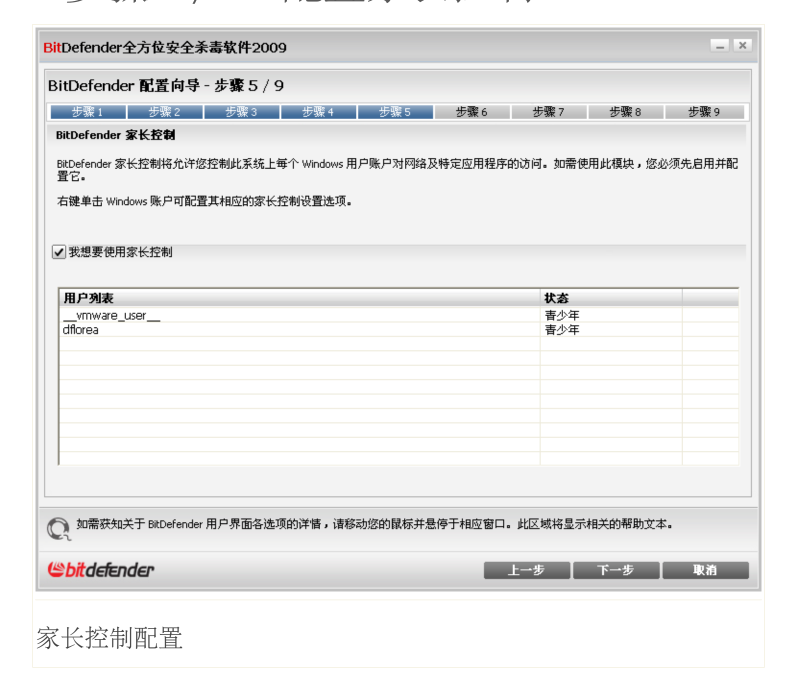
要添加例外，按照下列步骤进行：

1. 点击 添加 按钮添加一个新的条目。
2. 双击指定允许的地址，并输入您希望添加为例外的网址或电子邮件地址。
3. 双击选择类型，并从菜单中选择和之前输入的地址对应的类型。
   ■如果您指定的是一个网站地址，请选择HTTP。
   ■如果您指定的是一个电子邮件地址，请选择SMTP。

要删除一个例外，请选中它并点击 删除 按钮。

点击 确定 关闭窗口。

2.2.5. 步骤 5/9 –配置家长控制



家长控制配置

BitDefender家长控制，您可以控制使用互联网，并具体应用为每个用户持有一个用户帐户的系统。

如果您想要使用的家长控制，请执行下列步骤：

1. 选择我想使用家长控制 。
2. 右击名称每个Windows帐户并选择父母控制面板进行应用。

好处	说明
儿童	根据对14周岁以下用户的推荐设置,限制网页访问. 阻止含有对儿童可能有害内容的网页(色情、性、毒品、打杀等）.

好处	说明
少年	根据对14-18周岁用户的推荐设置,限制网页访问. 阻止所有关于性、色情作品或成人内容的网页.
成人	无论网页内容是什么,不限制访问所有网页.



注意

为了充分配置或禁用家长控制的具体的Windows帐户，启动BitDefender ，切换到高级视图和去家长控制. 你可以配置家长控制来阻止:

■不适当的网页。
■互联网接入，为特定的时间内（诸如时间节点） 。
■网页和电子邮件，如果他们含有某些关键字。
■应用，如游戏，聊天， filesharing程式或其他人。
■即时消息发送的即时消息联系人以外的其他允许的。

点击 下一步 继续。

2.2.6. 步骤 6/9 –配置病毒报告



病毒报告选项

BitDefender可以匿名发送在您计算机上发现的病毒到BitDefender实验室，以便追踪病毒爆发。

您可以配置下列选项：

■发送病毒报告 – 将在您计算机上发现的病毒发送给Bitdefender实验室。

■启用病毒爆发检测 – 将潜在的病毒爆发报告发送给Bitdefender实验室。



注意
该报告将不包含任何私密资料，如您的姓名或IP地址，也不会被用作商业用途。

点击 下一步 继续。

2.2.7. 步骤7/9 – 选择任务开始运行



任务选择

对BitDefender全方位安全杀毒软件进行设置,使其执行重要的任务以维护系统安全.您可选择以下任务:

■升级BitDefender反病毒2009引擎（可能需要重启电脑） – 在下一步中，将会对BitDefender反病毒2009引擎进行升级以保护您的计算机免受最新病毒侵害。

■运行快速系统扫描（可能需要重启电脑） – 在下一步中，将会运行快速系统扫描以保证您的 Windows 和 Program Files文件夹未受病毒感染。

■每天凌晨2点运行一次全面系统扫描 – 自动在每天早上2点运行一次全面系统扫描。

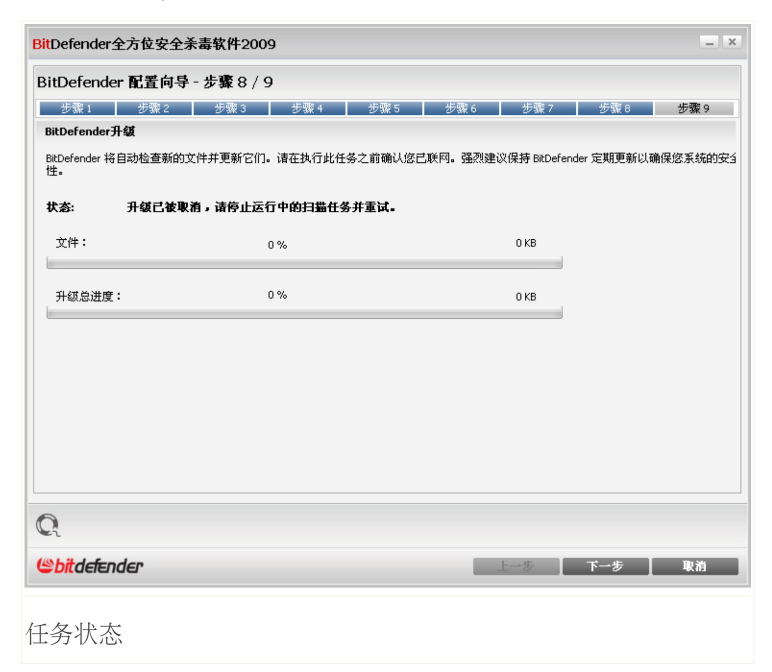


重要
为了确保您的系统安全，我们建议您在进入下一步之前启用这些选项。

如果您只选择最后一个选项或者未选择任何选项，您将跳过下一步。

点击 下一步 继续。

2.2.8. 步骤8/9–等待任务完成



任务状态

等待任务完成。您可以看到您在之前步骤中选择的任务的状态。

点击 下一步 继续。

2.2.9. 步骤9/9 –完成



完成

选择打开我的Bitdefender账户 进入您的Bitdefender账户，此操作需要联网。点击完成。

3. 升级

要添加计算机到bitdefender全方位安全杀毒软件，按照下列步骤进行：

1. 选项. 如果该版本的BitDefender包括反垃圾邮件，你可以选择储存朋友和垃圾邮件名单 ，以便以后使用它们。 欲了解更多信息，请参阅帮助文件或产品用户手册。
2. 删除您计算机上的老版Bitdefender。 欲了解更多信息，请参阅帮助文件或产品用户手册。
3. 重新启动计算机。
4. 安装BitDefender全方位安全杀毒软件中所描述的 “产品安装” (第 4 页)节本用户指南。

4. 修复和卸载BitDefender

如果你想改变、维修或拆除 BitDefender 全方位安全杀毒软件 按照Windows的开始菜单: 开始 ; → 程式; → BitDefender 2008 → 修改、修复或删除.

您将被要求按下下一步确认您的选择, 之后会出现一个新窗口供您选择:

■修复 – 重新安装上一次安装中所选的程序组件。

如果你选择修复BitDefender, 会显示一个新窗口。 点击修复 开始修复过程。

重新启动计算机时, 提示和后, 请按一下安装重新安装BitDefender全方位安全杀毒软件。

安装过程完成后, 会显示一个新窗口。 点击完成。

■卸载 – 卸载所有已经安装的组件。



注意
我们建议您选择 卸载 以进行一次干净的重装。

如果您选择卸载BitDefender, 会显示一个新窗口。



重要

通过消除bitdefender , 你将不再受到保护, 免遭病毒, 间谍软件和黑客的攻击。 If you want Windows Firewall and Windows Defender (only on Windows Vista) to be enabled after uninstalling BitDefender, select the corresponding check boxes.

点击 移除 开始拆除BitDefender 全方位安全杀毒软件。

在卸载过程中, 你将被提示向我们发送您的反馈。 请点击 确定 参加我们的在线调查, 仅有不超过五个小问题。 如果您不愿参加调查, 请点击 取消。

卸载过程完成后, 会显示一个新窗口。 点击完成。



注意
卸载结束后, 我们建议您删除位于 Program Files中的BitDefender 文件夹。

在卸载过程中发生错误

如果在卸载BitDefender过程中发生错误，卸载进程会中止，并显示一个新窗口。请点击 运行卸载工具 以确保BitDefender被完全删除。 卸载工具将会删除所有自动卸载过程没有删除的文件和注册表项。

基本管理

5. 开始使用

一旦您已经安装了Bitdefender，您的计算机就会受到保护。

5.1. Bitdefender全方位安全杀毒软件

要想让BitDefender发挥最大作用，第一步是启动它。

要访问BitDefender全方位安全杀毒软件主界面，请使用Windows “开始” 菜单，然后点击如下路径： 开始 → 程序 → BitDefender 2009 → BitDefender 全方位安全杀毒软件。或者采用更快方式，双击 BitDefender 系统托盘图标。

5.2. 用户界面视图

Bitdefender全方位安全杀毒软件会满足无论是非常技术性的人或电脑初学者的需要。因此，图形用户界面设计，以适应每一个类别的用户。

您可根据您对我们产品的熟悉程度选择要使用Bitdefender的基本视图或高级视图。



注意
您可以方便地在两个视图之间切换，只需点击 切换到基本视图 或 切换到高级视图 按钮即可。

5.2.1. 基本视图

基本视图的界面相对简单，让您可以设置所有模块的基本功能，你将能了解警告和严重警报，并修复问题。



基本视图

■您可以很容易发现在界面的上部有两个按钮和一个状态条。

项目	说明
设置	打开一个窗口，您可以轻松地启用或停用重要的安全模块（防火墙，隐身模式，自动更新，游戏模式，等等）。
切换到高级视图	打开高级视图窗口。在这里您可以看到全部模块，并可配置每个组件的细节。BitDefender会在您下次打开用户界面时记住这个选项。
状态	包含关于您系统安全漏洞的信息，并帮助您修复这些问题。

■在窗口中部有五个标签页。

标签页	说明
图表板	显示有用的产品统计和您的注册状态，以及启动重要的手动扫描任务的链接。

标签页	说明
安全	显示器安全模块状态（防病毒，反钓鱼，防火墙，反垃圾邮件，即时消息加密，隐私，漏洞检查和更新模块）连同联系的防毒软件，更新和脆弱性检查任务。
家长控制	显示状态的模块，使您可以限制孩子的接入互联网和具体应用。
文件管理器	显示文件状态去连接文件。
家庭网络	显示Bitdefender家庭网络结构。

■此外，Bitdefender基本视图窗口还包含一些有用的快捷方式。

快捷方式	说明
我的账户	让您创建或登录到您的Bitdefender账户。 Bitdefender账户可让您获得免费技术支持。
注册	您可在此输入新的授权密钥，或者查看当前授权密钥及注册状态。
帮助	打开帮助文件，帮助您了解如何使用Bitdefender。
技术支持	让您联络Bitdefender的支持团队。
历史记录	让您看到BitDefender在您计算机上执行的所有任务的详细历史信息。

5.2.2. 高级视图

高级视图让您可以访问BitDefender产品的每个组件，使用高级功能并配置高级的设置。





高级视图

■您可轻松发现窗口的上部有一个按钮和一个状态条。

项目	说明
切换至基本视图	打开基本视图窗口。在这里您可以看到包括主要模块（安全、系统优化、文件保险箱、家庭网络）的基本BitDefender界面以及一个图表板。BitDefender会在您下次打开主界面时记住此选项。
状态	包含关于您系统安全漏洞的信息，并帮助您修复这些问题。

■在窗口的左侧有一个包含所有安全模块的菜单。

模块	说明
常规	让您访问常规设置选项，或浏览图表板及系统信息。
反病毒	您可详细设置您的病毒防护和扫描操作选项，还可以设置扫描白名单和隔离区。
反垃圾邮件	让您保持您的收件箱中的垃圾邮件，并配置反垃圾设置细节。
防火墙	让您保护您的计算机从入站和出站擅自连接尝试。这是十分相似的后卫在您的大门–这将密切留意您的互联网连接和追踪是谁允许进入因特网。
隐私控制	防止您的数据被从您的计算机上窃取，并保护您的上网隐私。
家长控制	让您保护您的孩子对不适当的内容，使用您的个性化电脑准入规则。
加密	允许您加密雅虎和Windows Live （的MSN ） Messenger的通信。
漏洞检测	让您可以保持您计算机上关键软件处在最新版本。
游戏/笔记本模式	当您运行在笔记本电池时，推迟bitdefender计划任务；当您在玩游戏时，不显示警告及弹出窗口。
家庭网络	让您可以配置及管理家里多台计算机上的BitDefender产品。
升级	您可获取最新升级包，升级产品并配置升级过程的细节。
注册	允许您注册Bitdefender全方位安全杀毒软件，改变的授权码或创造一个bitdefender帐户。

■此外，Bitdefender高级视图窗口还包含几个有用的快捷方式。

快捷方式	说明
我的账户	让您创建或登录到您的Bitdefender账户。 Bitdefender账户可让您获得免费技术支持。
注册	您可在此输入新的授权密钥，或者查看当前授权密钥及注册状态。
帮助	打开帮助文件，帮助您了解如何使用Bitdefender。

快捷方式	说明
技术支持	让您联络Bitdefender的支持团队。
历史记录	让您看到BitDefender在您计算机上执行的所有任务的详细历史信息。

5.3. Bitdefender系统托盘图标

要想更快捷地管理本产品，您还可以使用Bitdefender系统托盘图标。

如果您双击此图标，BitDefender将主界面将会打开。此外，通过右键点击图标，将会显示上下文菜单，从而使您更快管理BitDefender产品。

打开 打开Bitdefender主界面。



Bitdefender系统托盘图标

-
- 帮助 – 打开帮助文件解释了Bitdefender全方位安全杀毒软件详细研究。
- 关于 – 打开Bitdefender “关于” 对话框。
- 修复所有问题 – 帮助您修复安全漏洞。
- 开启/关闭游戏模式 – 开启或关闭游戏模式。
- 立即更新 – 立即进行升级。 将会出现一个新窗口，显示升级状态。
- 设置 – 您可方便地启用或禁用重要的安全模块。 将会出现一个新窗口，您可在其中通过点击启用/禁用这些模块。

在游戏模式下，您可以看到字母 G 叠加在 BitDefender 系统托盘图标上。

如果有严重问题影响您的系统安全，会有一个感叹号显示在 BitDefender 系统托盘图标上。 你可以悬停鼠标在图标上看到影响您系统安全的问题数目。

5.4. 扫描活动条

扫描活动条 以图形化方式显示您系统上的扫描活动。



扫描活动条

灰色条（文件区域） 显示每秒扫描的文件数量，刻度从0到50。

在 网络区域 里的红色指标显示每秒转移的Kbytes数(从互联网上收发),规模从0到100.



注意
扫描活动标 将在相应的地区（档案区或网络区)打上红色的叉以通知你病毒屏障 或防火墙被停止了。这样,不打开管理介面你也可以知道你是否被保护。

您可以使用 扫描活动条 扫描文件，只需把文件拖放到扫描活动条上并放下即可。欲了解更多信息，请参阅 “拖放扫描” （第 146 页)。

当你不再想查看扫描活动条时，只需右键点击他然后选择 隐藏 即可。 要完全隐藏这个窗口，请执行下列步骤:

1. 点击 切换至高级视图 （如果您处在基本视图） 。
2. 从左侧菜单中点击常规 模块。
3. 点击 设置 标签。
4. 清除 启用扫描活动条（产品活动的图形化显示） 复选框。

5.5. Bitdefender手动扫描

如果你想快速扫描某一个文件夹，你可以用Bitdefender手动扫描。

要使用Bitdefender手动扫描，请从Windows开始菜单上，按以下路径点击：开始 → 程序 → BitDefender 2009 → Bitdefender手动扫描 就会出现下面的窗口：



Bitdefender手动扫描

您可浏览文件夹并选择您想扫描的文件夹，然后点击 确定。 BitDefender扫描程序 将会出现并引导您完成整个扫描过程。

5.6. 游戏模式

游戏模式会暂时改变防护设置，以减低它们对系统性能的影响。 在游戏模式下，会应用以下设置:

■尽量减少处理器占用时间与内存消耗

■推迟自动升级及扫描

■消除所有的警报和弹出窗口

■只扫描最重要的文件

在游戏模式下，您可以看到字母 G 叠加在 BitDefender 系统托盘图标上。

5.6.1. 使用游戏模式

如果您想开启游戏模式，请使用下列方法之一:

■右键点击系统托盘上的BitDefender图标，并选择开启游戏模式。

■按下Ctrl+Shift+Alt+G（游戏模式的默认快捷键）。



重要

在您结束游戏后别忘了关闭游戏模式，您可使用和开启游戏模式相同的方法关闭它。

5.6.2. 修改游戏模式热键

如果您想改变热键，请按照下列步骤：

1. 点击 切换至高级视图 （如果您处在基本视图）。
2. 点击左侧菜单上的 游戏/笔记本模式。
3. 点击游戏模式标签。
4. 点击高级设置按钮。
5. 在使用热键选项下面，设置您希望使用的热键：
   - 通过选中下面的功能键来设置热键：Ctrl键Ctrl，Shift键Shift，Alt键Alt。
   - 在编辑框中输入您想使用的普通键。

   例如，如果您想使用 Ctrl+Alt+D热键，您需要选中 Ctrl 和 Alt 并输入 D。



注意
取消选中 使用热键 旁的复选框将禁用热键。

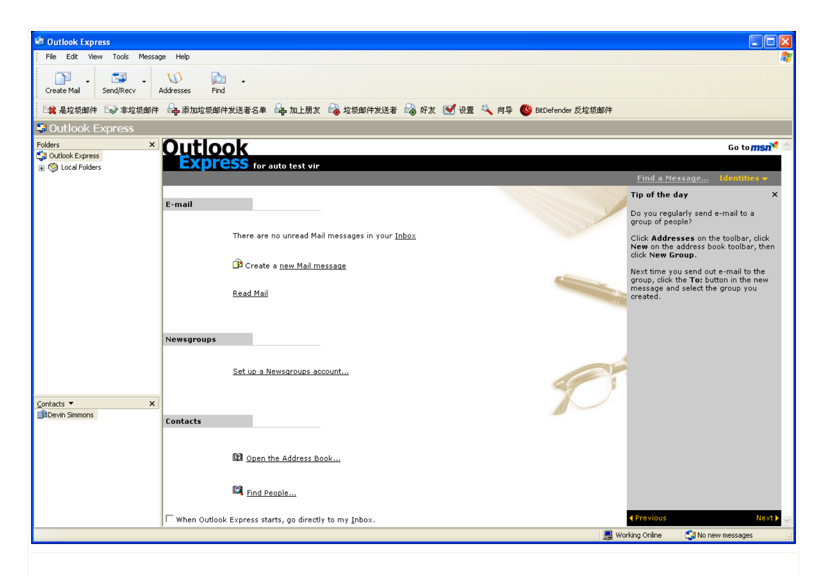
5.7. 集合到邮件客户端

BitDefender 集成直接地与Microsoft Outlook/Outlook Express 通过一个直觉和易使用的工具栏。

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

5.7.1. 反垃圾邮件工具栏

在Microsoft Outlook/Outlook Express 的顶边您能看Antispam 工具栏。



反垃圾邮件工具栏



重要

BitDefender Antispam 在Microsoft Outlook 或Outlook Express 的区别是，SPAM 消息被移动到 Spam 文件夹为Microsoft Outlook 当为Outlook Express 他们被移动被 Deleted Items 文件夹。在两个案件消息被标记作为SPAM 在附属的线。

Spam 文件夹由BitDefender 自动地创造在Microsoft Outlook 和是列出的在同样水平以项目从 文件夹目录(日历，联络等等) 。

BitDefender 工具栏中的每个按钮将被解释如下:

■ 是垃圾邮件 –发出了一个信息的贝叶斯模块表明，所选的电子邮件是垃圾邮件。电子邮件将标记为垃圾邮件并移至垃圾邮件文件夹。

以后同样的电子邮件样式将被标记为SPAM 。



注意

您能选择一个电子邮件或许多个电子邮件。

■ 这不是垃圾邮件 -发出了一个信息的贝叶斯模块表明，所选的电子邮件不是垃圾邮件BitDefender不应有标记它。电子邮件将是从文件夹收件箱目录。

以后同样的电子邮件样式将不再被标记为SPAM 。

注意
您能选择一个电子邮件或许多个电子邮件。



重要
The 非垃圾邮件 按钮便激活，当您选择一则消息由BitDefender被标记作为SPAM时(这些消息通常位于 Spam 文件夹)。

■ 自动添加到垃圾邮件列表 - 加发令者到 垃圾邮件列表



添加垃圾邮件发送者名单

选择不要再一次显示消息 如果您不想要被提示，当您添加垃圾邮件地址到名单。

点击 确定 关闭窗口。

以后从那个地址发出的电子邮件将被标记作为SPAM 。

注意
您能选择一个寄件人或许多个寄件人。

■ 添加到好友列表 - 加发令者到 好友列表





加上朋友

选择不要再一次显示这条消息 如果您不想要被提示，当您加朋友的地址到名单时。

点击 确定 关闭窗口。

您将收从这个地址收到邮件不管他们包含什么内容。



注意

您能选择一个寄件人或许多个寄件人。

■ 垃圾邮件发送者 – 打开 垃圾邮件发送者列表 包含所有不想接收其电子邮件的地址，而不管所包含的内容。



注意

任何一个电子邮件收到从地址包含在 垃圾邮件清单 自动地将被标记作为SPAM ，没有进一步处理。



垃圾邮件清单

您能补充说或从 垃圾邮件清单 去除词条。

如果您想要添加电子邮件，选择 电子邮件地址 选择，键入地址和点击按钮 。地址将出现在 垃圾邮件发送者列表.



重要

句法: name@domain.com.

如果您想要增加一个域，选择 域名 选项，键入域名并点击按钮 。域名将出现在垃圾邮件发送者列表.



重要

句法:

- @domain.com, *domain.com and domain.com – 所有收到的电子邮件从 domain.com 将被标记作为SPAM
- *domain* – –所有收到的电子邮件从 域（不论是否域名结尾）将被标记作为SPAM。
- *com – 所有收到的有域名结尾的电子邮件 com 将被标记作为SPAM。

输入电子邮件地址，从 Windows通讯录 / Outlook Express文件夹 到Microsoft Outlook / Outlook Express / Windows Mail选择合适的选项，从导入电子邮件地址从 下拉式选单。

Microsoft Outlook Express / Windows 微软Outlook Express /窗口邮件 一个新的窗口将出现在那里你可以选择该文件夹包含电子邮件地址，你要添加到 Microsoft Outlook Express / Windows 垃圾邮件 发送清单。选择它们，然后点击 Microsoft Outlook Express / Windows 选择

在这两个情况下电子邮件地址将出现在导入列表。选择指定的部分并点击 添加他们到垃圾邮件发送者列表. 如果您点击 所有电子邮件将加到名单上。

删除一个项目，从清单中，选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单，但公告：这是不可能收回。

使用 保存/ 载入 按钮保存/ 载入垃圾邮件列表 文件可以.bw1 引伸。

选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.

点击 应用 和 好的 保存和关闭 垃圾邮件清单。

- 好友 - 打开 好友清单 包含所有要接收其电子邮件的地址，而不管所包含的内容。



注意
任一邮件来自地址包含在 好友名单，自动地将被交付对您的Inbox 没有进一步处理。





朋友名单

您能补充说或从 好友名单 去除词条。

如果您想要加上电子邮件检查 Email address 选择，键入地址和点击⊠按钮 地址将出现在 友好列表



重要

句法: name@domain.com.

如果您想要增加域，选择 域名 选项，键入域名并点击 ⊠ 按钮。域名将出现在朋友列表.



重要

句法:

- @domain.com, *domain.com 和domain.com – –所有收到的电子邮件从 domain.com 将到达您的 收件箱 不管他们的内容如何;
- *domain* – –所有收到的电子邮件从 域（无论是否域名结尾）将到达您的 收件箱 不管他们的内容如何;
- *com – 所有收到的有域名结尾的电子邮件 com 将到达您的 收件箱 不管他们的内容如何;

输入电子邮件地址，从 Windows通讯录 / Outlook Express文件夹 到Microsoft Outlook / Outlook Express / Windows Mail选择合适的选项，从导入电子邮件地址从 下拉式选单。

Microsoft Outlook Express 一个新视窗将出现从您能选择包含电子邮件您想要加到 友好列表 的文件夹的地方。选择他们和点击 选择

在这两个情况下电子邮件地址将出现在导入列表。选择指定的部分并点击 添加他们到 朋友列表。如果您点击 所有电子邮件将增加到名单。

删除一个项目，从清单中，选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单，但公告：这是不可能收回。

使用 保存/ 载入按钮 保存文件好友列表 . 文件包含.bwl 例外.

选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.



注意

我们建议您将朋友的名字和电子邮件邮址加入 朋友名单. BitDefender不会拒绝这单内的邮址来信。所以，把朋友加入朋友名单能确保收到合法的邮件。

点击 应用 和 好的保存和关闭 好友列表

■ 设置 – 打开 设置 窗口，你可以为 反垃圾邮件 模块指定一些选项。



设置



您可选择以下任务:

- 移动信息删除的项目 –动作，垃圾邮件讯息给 删除的项目 （只适用于微软的Outlook Express/窗口邮件） ；
- 标记消息为 “已读” – 标记所有垃圾邮件消息为已读，这样不至于干扰新垃圾消息到达。

如果您的垃圾邮件过滤器是非常不精确的，您可能需要擦去滤器数据库和再培训 Bayesian 过滤器. 点击 擦去 antispam 数据库 重新设置贝 Bayesian 数据库.

使用 节省贝叶斯/ Load Bayes按钮以节省/负载该 贝叶斯数据库 名单，以理想的位置。该文件将有。.dat 延期。

点击 警报 页签，如果你想要访问这个单元，禁用确认窗口 添加垃圾邮件发送者 和 添加好友 按钮。



注意

在这个提醒窗口，您能开启/关闭的幻象。请选择一封电子邮件信息提醒.如果您选择了一组邮件信息,而不是一封的话,就会出现这个提醒窗口.

- 向导 – 打开 向导 指引你逐步训练 贝叶斯过滤器， BitDefender反垃圾邮件将逐步增加。 你也可以从 地址薄 添加地址到 好友清单 / 垃圾邮件发送者清单。
- BitDefender反垃圾邮件 – 打开 BitDefender用户界面。

5.7.2. 反病毒配置对话框

安装BitDefender后，第一次运行您的邮件客户端，将出现一个向导帮助您配置 好友清单 和 垃圾邮件发送者清单 并培训 贝叶斯过滤器 ，以便提高反垃圾邮件过滤器的效率。



注意

这个向导也可以在任何时候通过单击 向导 按钮启动，在 反垃圾邮件工具条。

步骤一 — 欢迎窗口



欢迎窗口

点击 下一步。

步骤2/6 – 填录好友名单

BitDefender - 反垃圾邮件向导

添加您的联系人至好友列表

步骤 1 | 步骤 2 | 步骤 3 | 步骤 4 | 步骤 5 | 步骤 6

您可以自动添加地址簿中的所有联系人至 "好友" 列表。

canalexecutivo.com@mcmatercarr.

全部选择

跳过此步骤

返回至上一页

bitdefender 上一步 下一步 取消

填录好友名单

您能看到所有的地址从您的 地址本。请选择那些您想要增加的到您的 朋友列表 (我们推荐选择他们全部) 。您将从这些地址全部接收邮件，不论它们的内容。

加上所有你接触到好友名单中，选中 全部选择.

选择 跳过这一步 如果您想要通过这步。点击 后退 回到早先步骤或点击 下一步继续向导。



步骤3/6 – 删除 Bayesian 数据库

删除 Bayesian 数据库

您可以发现您的垃圾邮件过滤器开始没有效率。这也许是因为不正当的训练(例如，即您错误地标记了一定数量合法的消息作为垃圾，或反之亦然） 。如果您的过滤器是非常不精确的，您可能需要清楚滤器数据库和再培训过滤器，通过接下来的向导。

选择 擦去垃圾邮件过滤器数据基础 如果您想要重新设置Bayesian数据基础。

使用 保存Bayes 或 装载Bayes 按钮来保存/装载Bayesian 数据基础 列表到一个指定的地点。文件将有 .dat 扩展名。

选择 跳过这一步 如果您想要通过这步。点击 后退 回到早先步骤或点击 下一步 继续向导。



步骤4/6 – 训练Bayesian 过滤以合法的电子邮件



训练Bayesian filter以合法的电子邮件

请选择包含合法电子邮件的一个文件夹。这些消息将用来训练垃圾邮件过滤器。

有两个高级选项下的目录清单：

■包括子文件夹 –包括子文件夹，以您的选择。
■自动添加到好友列表 – 加发令者到 好友列表

选择 跳过这一步 如果您想要通过这步。点击 后退 回到早先步骤或点击 下一步 继续向导。



步骤5/6 – 用垃圾邮件训练贝叶斯过滤器



训练Bayesian 过滤反垃圾邮件

请选择包含垃圾电子邮件的一个文件夹。这些消息将用来训练垃圾邮件过滤器。



重要
请确定，您选择的文件夹没有包含合法的电子邮件，否则防止垃圾邮件程序的表现将打折扣。

有两个高级选项下的目录清单：

■包括子文件夹 –包括子文件夹，以您的选择。
■自动添加到垃圾邮件列表 – 加发令者到 垃圾邮件列表

选择 跳过这一步 如果您想要通过这步。点击 后退 回到早先步骤或点击 下一步 继续向导。



步骤6/6 – 概要



扫描结果摘要

这里您能查看所有配置向导的设置。您可以返回上一步做任何修改(点击 后退).

如果您不想要做任何改动, 点击 完成 结束向导。

5.8. 集成到浏览器

Bitdefender在您上网时保护您免受钓鱼欺诈。 它扫描您浏览的网页, 并在发现钓鱼网站时提醒您。 您可以配置一个网站白名单, BitDefender将不会扫描白名单中的网站。

Bitdefender采用直观易用的工具条形式整合到下列的浏览器中:

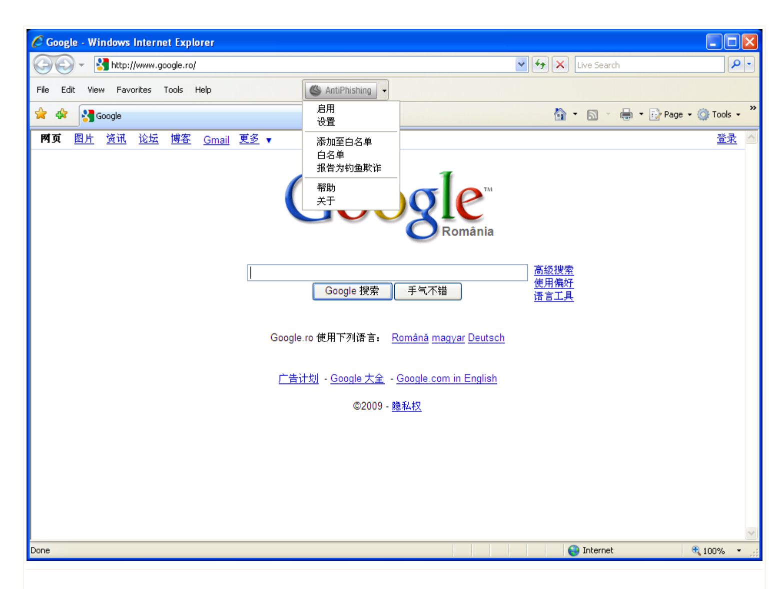
- Internet Explorer
- Mozilla Firefox

您可以通过集成到上述浏览器中的Bitdefender反钓鱼工具条方便地管理反钓鱼防护和网站白名单。

反钓鱼工具条，带有 Bitdefender图标，位于浏览器的顶部。 点击打开工具条菜单。



注意
如果您看不到工具条，请打开 视图 菜单，指向 工具栏 并选中 Bitdefender工具栏。



反钓鱼工具栏

工具栏包含下面的命令菜单：

■启用/禁用 Bitdefender反钓鱼工具栏。



注意
如果禁用反钓鱼工具栏，您将不再受到反钓鱼欺诈的保护。

■设置 – 打开饭店与工具栏的设置窗口进行选项设置。

您可选择以下任务：
・启用扫描 – 启用反钓鱼扫描。

· 添加白名单之前询问 – 当您添加网站到白名单时询问您。

■添加至白名单 – 添加当前网站到白名单。



注意

添加网站到白名单中后，Bitdefender将不会扫描该网站是否有钓鱼企图。我们建议您只添加您完全信任的网站到白名单中。

■查看白名单 – 打开白名单查看。

您可看到所有不会被Bitdefender反钓鱼引擎扫描的网站列表。

如果您要从白名单中删除一个网站以便在该网站存在钓鱼风险时得到警告，请点击移除 按钮。

您可以将您完全信任的网站添加到白名单中，从而让Bitdefender反钓鱼引擎跳过扫描这些网站。 要向白名单中添加网站，请在对应的编辑框中输入网址，然后点击 添加。

■帮助 – 打开帮助文件。

■关于 – 打开一个包含Bitdefender及支持信息的窗口。

5.9. 集成到即时通讯软件

Bitdefender提供针对雅虎通和MSN的加密功能，保护您在聊天时不被窃取私密信息。

默认情况下，如果满足下列条件，Bitdefender会加密您所有的聊天内容：

■您的聊天对象装有支持即时通讯加密的Bitdefender产品，并且启用了针对该即时通讯软件的加密功能。

■您和您的聊天伙伴使用雅虎通或MSN。



重要

如果您的聊天对象使用了网页聊天工具（如网页版雅虎通和MSN），或者其他支持雅虎通和MSN的软件，Bitdefender将不会加密聊天内容。

您可以通过聊天窗口上的Bitdefender工具栏轻松设置即时通讯加密功能。

点击工具栏，可以进行如下操作：

■永久性启用/禁用针对某个聊天对象的加密

■邀请某一个聊天对象使用加密

■从家长控制黑名单中删除某个聊天对象



即时通讯加密选项

只需点击一下上述的选项就可使用它。

6. 图表板

点击图表板标签，您会看到各类有用的统计信息，您的注册状态，以及指向重要手动扫描任务的链接。



图表板

6.1. 概览

在这里您可以看到有关升级状态、您的账号状态、注册及授权密钥的信息。

项目	说明
上次升级	显示您上次升级Bitdefender产品的日期，请定期升级以确保系统得到有效防护。
我的账户	显示您的电子邮件地址，您可用此地址登录您的在线账户，找回您丢失的BitDefender授权密钥，并获取技术及客户服务。

项目	说明
注册	显示您的授权密钥类型和状态。为确保您的系统安全，在密钥过期后请及时更新密钥。
将过期于	显示授权密钥过期的剩余天数。

要升级Bitdefender，请点击“任务”区域的 立即升级 按钮。

要创建或登录到您的Bitdefender账户，请按照下列步骤操作。

1. 点击窗口底部的 我的账户 链接，会打开一个网页。
2. 输入您的用户名和密码，并点击 登录 按钮。
3. 要创建一个BitDefender账户，请选择 You don't have an account? 并输入必要的信息。



注意
您在这里提供的信息都将保密。

注册BitDefender全方位安全杀毒软件，执行这些步骤。

1. 点击窗口底部的 我的账户 链接，会打开一步注册向导。
2. 点击 我想要使用新的密钥注册产品 单选按钮。
3. 在对应的文本框中输入新的授权密钥。
4. 点击完成。

要购买新的授权密钥，请按照下列步骤操作。

1. 点击窗口底部的 我的账户 链接，会打开一步注册向导。
2. 点击 更新您的Bitdefender授权密钥链接，会打开一个网页将。
3. 点击 现在购买 按钮。

6.2. 任务

在这里您可以找到指向重要安全任务的链接：全面系统扫描、深度系统扫描和升级。

下列按钮可用：

- 全面系统扫描 - 在您的计算机上运行全面扫描（不包含压缩文档）。
- 深度系统扫描 - 开始全面扫描您的计算机（包括压缩文档）。
- 立即升级 - 立即开始升级产品。

6.2.1. 用BitDefender扫描计算机

要在您的计算机上扫描恶意软件，请点击对应的按钮运行一个扫描任务。 下表介绍各个扫描任务：

任务	说明
全面系统扫描	扫描整个计算机，不扫描压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。
深度系统扫描	扫描整个系统，包括压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。



注意

由于深系统度扫描和全面系统扫描任务分析整个系统，扫描可能需要占用较长时间。因此，我们建议您用较低优先级运行这些任务，或在系统处于闲置状态是运行这些任务。

当您启用一个手动扫描进程后，无论是快速扫描或完整扫描，Bitdefender扫描程序就会出现。

请遵循向导程序的三个步骤来完成扫描过程。

6.2.2. 产品升级

每天都会发现新病毒，所以需要及时更新BitDefender病毒库。

默认情况下，Bitdefender在您启动计算机时会检查是否有可用升级，此后每个小时都会进行检查。 不过，如果您想自己更新Bitdefender，请按 立即升级。 升级进程会被启动，并显示下面的窗口：

BitDefender全方位安全杀毒软件2009

升级

BitDefender升级

BitDefender 将自动检查新的文件并更新它们。请在执行此任务之前确认您已联网。强烈建议保持 BitDefender 定期更新以确保您系统的安全性。

状态: 正在检查更新

文件： 0 % 0 KB

升级总进度： 37 % 0 KB

bitdefender 完成 取消

产品升级

在此窗口中您可以看到升级进程的状态。

升级过程是逐步执行的，需要被更新的文件会被逐步替换，因此升级过程不会影响产品的正常运行，同时又可减少系统漏洞。

如果您想关闭此窗口，请点击 取消。 不过，窗口关闭后并不会停止升级进程。



注意

如果您通过拨号方式连接到网络，建议您定期手动升级产品。

如果需要，请重启计算机。． 在进行了较大的升级后，您会被要求重启计算机。

点击 重启 会立即重启您的计算机。

如果您想稍后再重启，请点击确定。 我们建议您尽快重启您的计算机。

7. 安全性

BitDefender可以对必要的安全任务进行快捷扫描。运行这些任务时您可以更新BitDefender、扫描系统或阻止流量。

进入安全模式，再点击 安全 条目。



安全性

安全模块由两个部分：

- ■已监控组件 – 您可看到每个安全模块中被监控的所有组件。您可在此选择要监控的组件，建议您监控所有的组件。
- ■任务 – 您可在此找到指向重要安全任务的链接：全面系统扫描、深度系统扫描及立即升级。

7.1. 已监控组件

在监测的组成部分分为几类。

类别	说明
本地安全	您可在此找到保护您计算机中各类对象（文件、注册表、内存等）的各个安全模块的状态。
在线安全	在这里您可以检查所有保护您网上交易及上网计算机安全的各个模块的状态。
漏洞扫描	您可在这里检查您计算机上的关键软件是否为最新版本，同时还可根据安全规则检查Windows账户密码是否安全。

点击"+" 展开类别或点击"-"收起它。

7.1.1. 本地安全

我们知道它的重要的是要注意到，每当有问题，可能会影响您的计算机的安全性。通过监测每个安全模块， bitdefender全方位安全杀毒软件将可让您不知道，只有当您设定的设置，可能会影响您的计算机的安全，但是当你忘记这样做的重要任务。

影响本地安全的问题会用简单易懂的语言描述，如果需要您进行修改的话，在同一行还会有个红色的状态按钮 修复。 否则，将会心事一个绿色 确定 状态按钮

问题	说明
实时文件防护已启用	确保所有文件在被您或其他应用程序访问时被扫描。
您今天已经对系统进行了反有害软件扫描	强烈建议运行手动扫描以确保存储在您计算机上的文件没有被恶意软件感染。
自动升级已启用	请启用自动升级以确保病毒库定时获得更新。
立即升级	正在升级产品及病毒库。
防火墙已启用	保护您的计算机不受黑客和恶意软件的攻击。

如果状态按钮显示为绿色，则您系统的安全风险很小。要把按钮变为绿色，请执行以下步骤:

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

7.1.2. 在线安全

可能影响在线安全的问题用简单易懂的句子描述。如果某些问题影响到了计算机安全，您会看待一个红色的状态按钮 修复。 否则，将会心事一个绿色 确定 状态按钮

问题	说明
反垃圾邮件已启用	确保您的电子邮件扫描恶意软件和过滤的垃圾邮件已启用。
身份识别控制已启用	可以帮助您机密数据的安全扫描特定字符串的所有网页和电子邮件通信。这是建议，以使身份控制让您的机密数据（ e -mail地址，用户ID ，密码，信用卡号码等）的安全而不被偷走。
Firefox反钓鱼保护已启用	Bitdefender在您上网时保护您免受钓鱼欺诈。
Internet Explorer反钓鱼保护已启用	Bitdefender在您上网时保护您免受钓鱼欺诈。

如果状态按钮显示为绿色，则您系统的安全风险很小。要把按钮变为绿色，请执行以下步骤:

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

7.1.3. 漏洞扫描

可能影响漏洞检测的问题都以简单明了的描述列出，如果有影响您计算机安全的问题，在其后会显示一个红色的状态按钮 修复。 否则，将会心事一个绿色 确定 状态按钮

问题	说明
漏洞检测已启用	监控Windows更新、Office更新及Windows账户密码，以确保您的操作系统已经安装了最新补丁，同时密码不会被轻易攻破。
Microsoft关键更新	安装可用的Microsoft关键更新。

问题	说明
Microsoft其他更新	安装可用的Microsoft非关键更新。
Windows自动更新已启用	在新的Windows安全更新可用时第一时间安装它们。
管理员（强密码）	表明某个账户的密码强度。

如果状态按钮显示为绿色，则您系统的安全风险很小。要把按钮变为绿色，请执行以下步骤：

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

7.2. 任务

在这里您可以找到指向重要安全任务的链接：全面系统扫描、深度系统扫描和升级。

下列按钮可用：

- 全面系统扫描 – 在您的计算机上运行全面扫描（不包含压缩文档）。
- 深度系统扫描 – 开始全面扫描您的计算机（包括压缩文档）。
- 扫描“我的文档” – 扫描“我的文档”目录。
- 立即升级 – 立即开始升级产品。
- 漏洞检测

7.2.1. 用BitDefender扫描计算机

要在您的计算机上扫描恶意软件，请点击对应的按钮运行一个扫描任务。 下表介绍各个扫描任务：

任务	说明
全面系统扫描	扫描整个计算机，不扫描压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。

任务	说明
深度系统扫描	扫描整个系统，包括压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。
扫描“我的文档”	此任务将扫描当前用户的重要文件夹：我的文档 桌面和 启动项。 这将确保您的文档和工作环境安全，并保证开机启动程序是无毒的。



注意
由于深系统度扫描和全面系统扫描任务分析整个系统，扫描可能需要占用较长时间。因此，我们建议您用较低优先级运行这些任务，或在系统处于闲置状态是运行这些任务。

当您启用一个手动扫描进程后，无论是快速扫描或完整扫描，Bitdefender扫描程序就会出现。 请遵循向导程序的三个步骤来完成扫描过程。

7.2.2. 产品升级

每天都会发现新病毒，所以需要及时更新BitDefender病毒库。

默认情况下，Bitdefender在您启动计算机时会检查是否有可用升级，此后每个小时都会进行检查。 不过，如果您想自己更新Bitdefender，请按 立即升级。 升级进程会被启动，并显示下面的窗口：



BitDefender全方位安全杀毒软件2009

升级

BitDefender升级

BitDefender 将自动检查新的文件并更新它们。请在执行此任务之前确认您已联网。强烈建议保持 BitDefender 定期更新以确保您系统的安全性。

状态: 正在检查更新

文件： 0 % 0 KB

升级总进度： 37 % 0 KB

bitdefender 完成 取消

产品升级

在此窗口中您可以看到升级进程的状态。

升级过程是逐步执行的，需要被更新的文件会被逐步替换，因此升级过程不会影响产品的正常运行，同时又可减少系统漏洞。

如果您想关闭此窗口，请点击 取消。 不过，窗口关闭后并不会停止升级进程。



注意

如果您通过拨号方式连接到网络，建议您定期手动升级产品。

如果需要，请重启计算机。. 在进行了较大的升级后，您会被要求重启计算机。

点击 重启 会立即重启您的计算机。

如果您想稍后再重启，请点击确定。 我们建议您尽快重启您的计算机。

7.2.3. 检测漏洞

漏洞检测检查微软Windows更新、Office更新和您Windows账户密码，以确保您的操作系统安装了最新更新，同时您的密码不会被轻易攻破。

要检查您电脑的安全漏洞，请点击漏洞检测，并按照向导的步骤执行。

步骤 1/6 – 选择要检测的漏洞



漏洞检测

点击 下一步 在系统中检查所选的漏洞。

步骤 2/6 – 检测漏洞



漏洞检测

请等待Bitdefender完成漏洞检测。

步骤 3/6 – 修改弱密码



用户密码

您可以看到您计算机上的Windows用户账户列表，以及每个账户的密码强度。点击 修复 修改弱密码。 接着会显示一个新窗口。

BitDefender

Choose method to fix:

- Force user to change password at next login
- Change user password

Type password:

Confirm password:

OK Close

修改密码

选择修复此问题的方法:

■强制用户在下次登录时修改密码. Bitdefender会在用户下次登录Windows时提示用户更改密码。

■更改用户密码. 您必须在编辑框输入新密码。



注意
强密码是指组合了大写和小写字母、数字及特殊字符（#、$ 和 @）的密码。

点击确认 修改密码。

点击 下一步。

步骤 4/6 – 更新应用程序



应用程序

您可看到BitDefender所检查的应用程序，以及它们是否最新版本。 如果应用程序不是最新版本，请点击后面的链接下载最新版本。

点击 下一步。



步骤 5/6 – 更新Windows



更新Windows

您可看到您的计算机上尚未安装的Windows关键及非关键更新列表。 点击 安装所有系统更新 要安装所有可用更新。

点击 下一步。

步骤 6/6 – 查看结果



查看结果

点击 关闭。

8. 家长

BitDefender配备父母模块可以帮助您

进入家长模式，再点击 家长 条目。



家长

家长模块包含两个部分：

■已监控组件 – 您可看到每个安全模块中被监控的所有组件。您可在此选择要监控的组件，建议您监控所有的组件。

■任务 – 您可在此找到指向重要安全任务的链接：全面系统扫描、深度系统扫描及立即升级。

8.1. 已监控组件

已监测组件有如下几个：

类别	说明
家长控制	你可以在此检查父母控制，使您可以限制孩子的上网和具体应用。

点击"+" 展开类别或点击"–"收起它。

8.1.1. 家长控制

家长控制的模块，使您可以限制接入互联网和具体应用。

问题当地的安全所描述的很清晰的句子。在符合每个句子，如果有一些可能会影响您的计算机的安全性，您会看到一个红色按钮，所谓的地位修复. 否则，将会心事一个绿色 确定 状态按钮

问题	说明
家长控制没有被配置	BitDefender父母控制单元能阻挡你认为不合适的网站，在某一段时期阻止连接互联网 （如上课时间)还可以阻止应用程式如游戏、聊天、文件分享程式等。

当状态的按钮是绿色，安全的风险，您的系统是在最低限度。把绿色按钮，请执行下列步骤：

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

8.2. 任务

在这里您可以找到指向重要安全任务的链接：全面系统扫描、深度系统扫描和升级。

下列按钮可用：

- 全面系统扫描 – 在您的计算机上运行全面扫描（不包含压缩文档）。
- 深度系统扫描 – 开始全面扫描您的计算机（包括压缩文档）。
- 立即升级 – 立即开始升级产品。

8.2.1. 用BitDefender扫描计算机

要在您的计算机上扫描恶意软件，请点击对应的按钮运行一个扫描任务。 下表介绍各个扫描任务：

任务	说明
全面系统扫描	扫描整个计算机，不扫描压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。
深度系统扫描	扫描整个系统，包括压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。



注意
由于深系统度扫描和全面系统扫描任务分析整个系统，扫描可能需要占用较长时间。因此，我们建议您用较低优先级运行这些任务，或在系统处于闲置状态是运行这些任务。

当您启用一个手动扫描进程后，无论是快速扫描或完整扫描，Bitdefender扫描程序就会出现。

请遵循向导程序的三个步骤来完成扫描过程。

8.2.2. 产品升级

每天都会发现新病毒，所以需要及时更新BitDefender病毒库。

默认情况下，Bitdefender在您启动计算机时会检查是否有可用升级，此后每个小时都会进行检查。 不过，如果您想自己更新Bitdefender，请按 立即升级。 升级进程会被启动，并显示下面的窗口：

BitDefender全方位安全杀毒软件2009

升级

BitDefender升级

BitDefender 将自动检查新的文件并更新它们。请在执行此任务之前确认您已联网。强烈建议保持 BitDefender 定期更新以确保您系统的安全性。

状态: 正在检查更新

文件： 0 % 0 KB

升级总进度： 37 % 0 KB

bitdefender 完成 取消

产品升级

在此窗口中您可以看到升级进程的状态。

升级过程是逐步执行的，需要被更新的文件会被逐步替换，因此升级过程不会影响产品的正常运行，同时又可减少系统漏洞。

如果您想关闭此窗口，请点击 取消。 不过，窗口关闭后并不会停止升级进程。



注意

如果您通过拨号方式连接到网络，建议您定期手动升级产品。

如果需要，请重启计算机。． 在进行了较大的升级后，您会被要求重启计算机。

点击 重启 会立即重启您的计算机。

如果您想稍后再重启，请点击确定。 我们建议您尽快重启您的计算机。

9. 档案库

BitDefender可以对必要的安全任务进行快捷扫描。运行这些任务时您可以更新BitDefender、扫描系统或阻止流量。

档案库. 您一定希望您的敏感文件远离窥探。这是文件管理器模块来处理。

- 文件是一个担保的存储空间的个人信息或敏感文件。
- 文件是一个加密文件中，您的计算机上与bvd延伸。
- 因为它是加密的数据在里面是无懈可击。
- 当您安装此bvd的文件，一个新的逻辑分区（一个新的驱动器）会出现。这将是您更容易了解这一过程，如果你认为类似一：安装ISO映像作为虚拟光盘。

只需打开我的电脑，你将看到一个新的驱动器。您将能够做的文件操作上（复制，删除，修改等） 。这些档案的保护，只要他们居住在这个驱动器（因为密码是需要安装操作） 。 完成后便开始保护其内容。

进入文件管理模块，请点击 文件 条目。



档案库

■监测元件–让您看到的完整清单监测元件为每个安全模块。您可以选择的模块加以监测。这是建议，使监测的所有组件。

9.1. 已监控组件

已监测组件有如下几个:

类别	说明
文件	这是一个有担保的存储空间的个人信息或敏感文件。这是在您的计算机。因为它是加密的数据里面是无懈可击，以偷窃或违背安全。

点击"+" 展开类别或点击"–"收起它。

9.1.1. 文件保护:

问题当地的安全所描述的很清晰的句子。在符合每个句子，如果有一些可能会影响您的计算机的安全性，您会看到一个红色按钮，所谓的地位修复. 否则，将会心事一个绿色 确定 状态按钮

问题	说明
文件隐藏已启用	档案库让您的文件加密特殊的驱动器。

当地位的按钮是绿色，安全的风险，您的系统是在最低限度。把绿色按钮，请执行下列步骤:

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

9.2. 任务

下列按钮可用:

■添加你的文件–开始程序，让您可以永久删除档案。
■删除文件–启动向导，使您可以删除数据。

■浏览–启动向导，允许您查看内容。
■锁–启动向导，使您可以锁定您的资料，以便开始保护其内容。

9.2.1. 新增文件

该文件是一个特殊的地方是用来储存宝贵的东西。该文件从一个文件是加密的形成。通过点击启动添加文件向导将带您完成整个过程，恢复你的备份数据。

步骤1/6— 选择对象

在这里您可以将指定的文件或文件夹添加到加密区。



对象

点击添加对象， 选择所需的文件或文件夹并点击好的。 路径选定的位置将出现路径，。 如果您改变位置，只要按一下删除"按钮。



注意
您可以选择其中一个或数个地点。

点击 下一步。

步骤2/6- 选择Vault

在这里您可以创建一个新区或选择一个已创建的区



选择库

如果您选择 浏览一个文件库你必须点击 浏览并且选择文件库.你可能进入第5步,直接进入该区,如果该区有锁,会进入第4步

如果您点击选择一个现有的文件库,您你必须先键如库名.如果您选择的区可以创建,那您会进入第5步.如果该区被锁了那您会进入第4步

选择创建一个新的文件库 如果没有一个现有的文件库适合你的需要.你会进入第3步

点击 下一步。

第6步/ 6 –创建库

这是您可以指定信息的新文件库



创建库

完全这个窗口的相关信息，请执行下列步骤:

1. 点击 浏览 选择一个当地的 bvd文件



注意

请记住,该文件库在您的计算机上是一个加密的文件bvd 延长.

2. 从相应的菜单中选择一个盘符作为新的文件库



注意

请记住,当你登上bvd 文件,一个新的分区(一个新的驱动)将会出现.

3. 在相应的领域,输入您的文件库密码。



注意
密码应该至少8字节长。

4. 请再输入一次密码
5. 设置文件库的大小,(以MB)输入进相应的地方



注意
大小只包含数字

点击 下一步。

你将会进入第五步

第3/ 6 步–密码

系统将会要求您为选定的文件库输入密码



输入密码

在相应的地方输入密码,单击下一步)

步骤6/6 – 概述

在这里您可以复查选择的项目



扫描结果摘要

点击 下一步。

第6/ 6步–查看结果

在这里你可以检查看文件库的具体内容。



查看结果

点击完成。

9.2.2. 删除文件库的文件

通过点击删除文件库的文件向导将引导您完成从特定文件库删除文件的过程.

步骤1/5— 选择文件库

在这里您可以选定一个需要删除文件的文件库



选择库

如果您选择 浏览并寻找文件保险箱，你必须点击浏览 并选择文件保险箱。 如果所选文件保险箱已经打开，您将进入步骤3，如果所选文件保险箱被上锁，您将进入步骤2.

如果你点击选择一个现有的文件库,然后,你必须点击所需要的文件库名.如果选择的文件库被打开你将会进入第3步.如果被锁定了,那么你将进入第2步

点击 下一步。

第2/ 5步 –密码

系统将会要求您为选定的文件库输入密码



输入密码

在相应的地方输入密码,单击下一步)

步骤3 / 5 –选择文件

在这里,您将提供从之前选择的文件库里的名单





选择文件

点击你想删除的文件，并点击下一步.。

第4/5步一 概要

在这里您可以复查选择的项目





扫描结果摘要

点击 下一步。

第6/ 6步 –查看结果

这是您可在此找到其中最重要的安全任务的链接.



查看结果

点击完成。

9.2.3. 永久删除档案

通过点击查看文件库向导将带您完成整个过程。

步骤1/4— 选择文件库

在这里你可以选择一个文件库，查看文件的位置。





选择库

如果您选择 浏览并寻找文件保险箱，你必须点击浏览 并选择文件保险箱。 如果所选文件保险箱已经打开，您将进入步骤3，如果所选文件保险箱被上锁，您将进入步骤2.

如果你点击选择一个现有的文件库,然后,你必须点击所需要的文件库名.如果选择的文件库被打开你将会进入第3步.如果被锁定了,那么你将进入第2步

点击 下一步。

第2/4–密码

系统将会要求您为选定的文件库输入密码





输入密码

在相应的地方输入密码,单击下一步)

步骤3/4–摘要

在这里您可以复查选择的项目





扫描结果摘要

点击 下一步。

第4/ 4步-查看结果

在这里您可以查看文件库的文件



查看结果

点击完成。

9.2.4. 文件库加密

文件库在您的电脑上都是加密的bvd.文件库可以是开放式的或有密码的.

为了更好的认识这个过程.试想一个真正的银行金库,它有一个可以开关的超坚硬的门.然而,文件库的内容只有被锁定时才能受到保护.同时,文件内容只有被打开是才能被看到.

通过点击文件夹上锁向导将带您完成整个过程.

步骤1/3— 选择文件库

在这里你可以指定想要加密的文件库.



选择库

如果您选择浏览一个文件库 你必须点击 浏览并选择文件库.

如果您单击 选择一个现有的文件库 然后你必须点击文件库名。

点击 下一步。

第2/3步— 概述

在这里您可以复查选择的项目



扫描结果摘要

点击 下一步。

第3/3步— 查看结果

这是您可在此找到其中最重要的安全任务的链接.



BitDefender 2009
文件保险箱 - 锁定保险箱
步骤 1
步骤 2
步骤 3
显示操作结果
操作
关闭保险箱
名称
fvtest2
路径
G:\scripts_v12\Testbed\FileVault\fvtest2.bvd
结果
操作成功。
错误代码
信息
保险箱文件已被成功锁定。
前进至向导中下一个步骤。
bitdefender
完成

查看结果

点击完成。

10. 家庭网络

家庭网络模块可让您从一台计算机上管理你家里所有计算机上的Bitdefender产品。要进入进入家庭网络模块，请点击家庭网络 标签。



家庭网络

要管理安装在您家里各台计算机上的Bitdefender产品，请按照下列步骤进行：

1. 在您的计算机上加入Bitdefender家庭网络。 加入家庭网络需要为家庭网络管理设置一个管理员密码。
2. 将每台您希望管理的计算机加入家庭网络（设定密码）。
3. 回到您的计算机，并将所有你希望管理的计算机加入家庭网络。

10.1. 任务

一开始，只有一个可用的按钮。



■加入/创建网络 – 您可设置家庭网络密码，从而加入网络。

加入家庭网络后，将会显示更多按钮。

■离开网络 – 离开家庭网络。
■管理网络 – 添加计算机到您的家庭网络。
■扫描全部 – 同时扫描所有您管理的计算机。
■升级全部 – 升级您所管理的所有计算上的BitDefender产品。
■注册全部 – 同时注册您管理的所有计算机上的BitDefender产品。

10.1.1. 加入家庭网络

要加入家庭网络，请按照下列步骤进行：

1. 点击 加入/创建网络。 系统会提示您设置家庭网络管理密码。



设定密码

2. 请在两个编辑框输入相同的密码。
3. 点击 确定。

您将看到计算机名出现在家庭网络地图中。

10.1.2. 向家庭网络中添加计算机

在添加计算机到家庭网络之前，您必须为每台计算机配置Bitdefender家庭管理密码。

要添加计算机到bitdefender家庭网络，请按照下列步骤进行：

1. 点击 管理网络。 系统会提示您输入家庭网络管理密码。



输入密码

2. 请输入家庭网络管理密码并点击 确定。 接着会显示一个新窗口。



添加计算机

您可看到家庭网络中所有计算机的列表。 图标含义如下:

表示一台在线但是没有安装Bitdefender产品的电脑。

表示一台在线并且安装了Bitdefender产品的电脑。

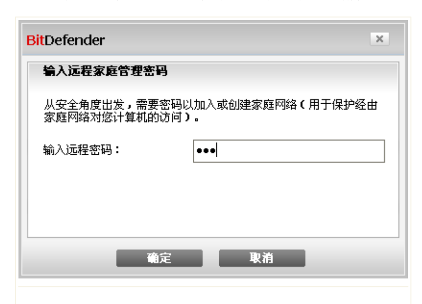
■ 表示一台离线的安装了Bitdefender产品的电脑。

3. 请执行如下操作之一：

■从列表中选择计算机名称加入。

■在对应区域输入要加入的计算机的IP地址或计算机名称。

4. 点击 添加。 系统会提示您输入该计算机的家庭网络管理密码。



权限验证

5. 输入在该计算机上设置的家庭网络管理密码。

6. 点击 确定。 如果您提供了正确的密码，选定计算机的名称会出现在家庭网络图中。



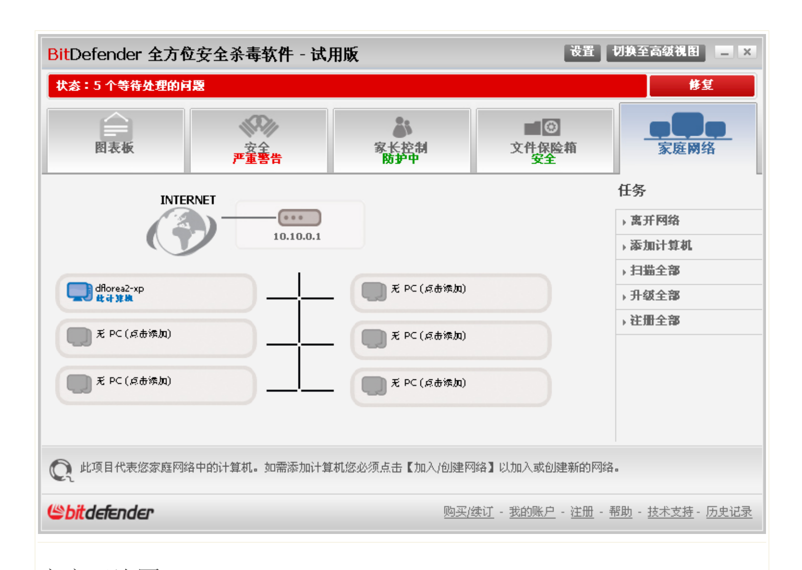
注意

您可以添加多达五台电脑到网络中。

10.1.3. 管理家庭网络

成功创建了Bitdefender家庭网络之后，您可以从一台计算机上管理所有计算机上的BitDefender产品。





家庭网络图

移动鼠标光标到网络图中的一台计算机上，您可以看到该计算机的简要信息（名称、IP地址、影响系统安全的问题数、注册状态等）。

右键点击网络图中的一个计算机名，您会看到所有在该计算机上可以执行的管理任务。

■注册此计算机

■设置配置密码。

■运行扫描任务

■修复此计算机上的问题

■查看此计算机的历史记录

■立即在此计算机上运行升级

■应用策略

■在此计算机上运行系统优化

■将此计算机设置为本网络的升级服务器

在某台计算上运行任务之前，系统会提示您输入家庭网络管理密码。



输入密码

请输入家庭网络管理密码并点击 确定。



注意

如果您计划执行多项任务，您可选择本次操作期间不要再次显示此消息。 选择此选项，您在本次操作期间将将不会再次被提示输入密码。

10.1.4. 扫描所有计算机

扫描所有您管理的计算机，请按照下列步骤:

1. 点击 扫描全部。 系统会提示您输入家庭网络管理密码。

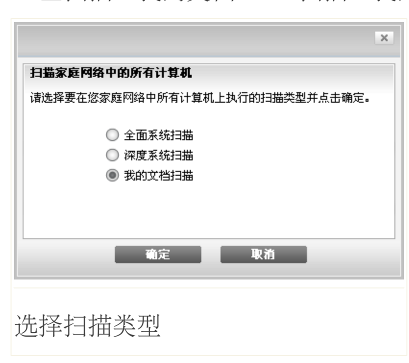
BitDefender
您必须输入家庭管理密码。
密码
本次操作期间不要再次显示此消息。
确定 取消

输入密码

2. 选择扫描类型。



■全面系统扫描 – 在您的计算机上运行全面扫描（不包含压缩文档）。
■深度系统扫描 – 开始全面扫描您的计算机（包括压缩文档）。
■扫描“我的文档” – 扫描“我的文档”目录。



选择扫描类型

3. 点击 确定。

10.1.5. 更新所有计算机

要升级所有您管理的计算机，请按照下列步骤:

1. 点击 升级全部。 系统会提示您输入家庭网络管理密码。



输入密码

2. 点击 确定。

10.1.6. 注册所有计算机

注册所有您管理的计算机，请按照下列步骤:

1. 点击注册全部。 系统会提示您输入家庭网络管理密码。



输入密码

2. 输入您要注册的授权密钥。



注册全部

3. 点击 确定。

11. 基本设置

您可在基本设置模块方便地启用/禁用重要的安全模块。

要进入基本设置模块中，请在基本视图的上方点击 设置 按钮。



基本设置

可设置的安全模块被分为三个类别。

类别	说明
本地安全	您可在此启用/禁用实时文件防护或自动升级。
在线安全	您可在此启用/禁用实时邮件和网页防护。
家长控制设置	这里您可以启用/禁用家长控制
网络安全	这里您可以启用/禁用防火墙。
常规设定	您可在此启用/禁用游戏模式、笔记本式、配置密码、扫描活动条及更多其他设置。

点击"+" 展开类别或点击"–"收起它。

11.1. 本地安全

您可以轻松点击鼠标就可启用/禁用安全模块。

安全模块	说明
实时防护病毒及间谍软件	实时文件防护确保任何文件在被您或计算机上的其他应用程序访问时被扫描。
自动升级	自动升级确保最新的BitDefender产品及病毒库文件被定时下载并安装。
自动漏洞检测	自动漏洞检测确保您计算机上的关键软件是最新版本。

11.2. 在线安全

您可以轻松点击鼠标就可启用/禁用安全模块。

安全模块	说明
实时防病毒与反间谍,反钓鱼邮件保护	实时邮件保护确保你的电子邮件经过垃圾邮件过滤和扫描钓鱼企图.
实时防毒与反间谍保护	实时网络保护确保所有下载的文件通过HTTP扫描钓鱼攻击。
实时反钓鱼网页防护	实时反钓鱼网页防护确保所有通过HTTP协议下载的文件都被扫描是否有钓鱼风险。
隐私控制	隐私控制通过在所有的网页及电子邮件流量中扫描特定字符串，保证您的私密信息安全。
即时通讯加密	如果您的聊天网友安装了BitDefender 2009，则你们之间通过雅虎通和MSN的的所有即时通讯会话都会被加密。

11.3. 家长控制设置

您可以通过点击来启用/禁用家长控制模块。

家长控制可以阻止进入不适当的网页或网络.它可以过滤电子邮件，即时通信和网络流量的上特定的字词。

11.4. 网络设置

您可以通过点击来启用/禁用防火墙模块。

防火墙保护您的计算机不受黑客和恶意的外界攻击

11.5. 文件库设置

您可以通过点击来启用/禁用文件库模块。

档案库让您的文件加密特殊的驱动器。

11.6. 常规设置

您可以通过鼠标点击轻松启用/禁用安全有关的项目。

项目	说明
游戏模式	游戏模式暂时修改防护设置，以尽量减少在玩游戏时对系统性能的影响。
笔记型电脑模式	笔记本电脑模式临时修改防护设置，以尽量减少对笔记本电脑电池的消耗。
配置密码	配置密码确保BitDefender的设置选项只能由知道密码的人修改。
家长控制密码	通过启用此选项，您将限制保护设置的家长控制模块。这确保了BitDefender家长控制设置只能由知道这个密码的人修改。
Bitdefender资讯	启用此选项，您将收到来自BitDefender的重要的公司新闻、产品更新或新的安全威胁信息。
产品通知警告	启用此选项，您将收到信息警报。
扫描活动状态条	扫描活动状态栏是一个很小的、透明的的工具条，显示Bitdefender的扫描活动。绿色线图显示您本地系统的扫描活动，红色线图显示您联网时的网络扫描活动。
启动时加载BitDefender	启用此选项， Bitdefender的用户界面将在系统启动时加载。此选项不影响防护级别。

项目	说明
发送病毒报告	启用此选项，病毒扫描报告将会被发送给Bitdefender实验室进行分析。请注意，这些报告将不包含机密资料，如您的姓名或IP地址，也不会被用作商业用途。
病毒爆发检测	启用此选项，有关潜在病毒爆发的报告会被发送到Bitdefender实验室进行分析。请注意，这些报告将不包含机密资料，如您的姓名或IP地址，也不会被用作商业用途。

12. 状态栏

在上半部分Bitdefender全方位安全杀毒软件的窗口有一个状态栏,显示目有待解决的问题数目。点击解决所有问题按钮来轻松消除任何威胁到您的电脑安全的程序。一个安全窗口将会出现。

安全状况显示计算机上的安全漏洞,那将是系统的有组织的并且容易管理的。bitdefender全方位安全杀毒软件将让你知道，每一个可以影响到你的计算机的安全性的问题。



状态栏

12.1. 本地安全

我们知道它的重要的是要注意到，每当有问题，可能会影响您的计算机的安全性。通过监测每个安全模块， bitdefender全方位安全杀毒软件将可让您不知道，只有当您设定的设置，可能会影响您的计算机的安全，但是当你忘记这样做的重要任务。

影响本地安全的问题会用简单易懂的语言描述，如果需要您进行修改的话，在同一行还会有个红色的状态按钮 修复。 否则，将会心事一个绿色 确定 状态按钮

问题	说明
实时文件防护已启用	确保所有文件在被您或其他应用程序访问时被扫描。
您今天已经对系统进行了反有害软件扫描	强烈建议运行手动扫描以确保存储在您计算机上的文件没有被恶意软件感染。
自动升级已启用	请启用自动升级以确保病毒库定时获得更新。
立即升级	正在升级产品及病毒库。
防火墙已启用	保护您的计算机不受黑客和恶意软件的攻击。

如果状态按钮显示为绿色，则您系统的安全风险很小。要把按钮变为绿色，请执行以下步骤:

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

12.2. 在线安全

可能影响在线安全的问题用简单易懂的句子描述。如果某些问题影响到了计算机安全，您会看待一个红色的状态按钮 修复。 否则，将会心事一个绿色 确定 状态按钮

问题	说明
反垃圾邮件已启用	确保您的电子邮件扫描恶意软件和过滤的垃圾邮件已启用。
身份识别控制已启用	可以帮助您机密数据的安全扫描特定字符串的所有网页和电子邮件通信。这是建议，以使身份控制让您的机密数据（e-mail地址，用户ID ，密码，信用卡号码等）的安全而不被偷走。
Firefox反钓鱼保护已启用	Bitdefender在您上网时保护您免受钓鱼欺诈。
Internet Explorer反钓鱼保护已启用	Bitdefender在您上网时保护您免受钓鱼欺诈。

如果状态按钮显示为绿色，则您系统的安全风险很小。要把按钮变为绿色，请执行以下步骤:

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

12.3. 文件保护:

问题当地的安全所描述的很清晰的句子。在符合每个句子，如果有一些可能会影响您的计算机的安全性，您会看到一个红色按钮，所谓的地位修复. 否则，将会心事一个绿色 确定 状态按钮

问题	说明
文件隐藏已启用	档案库让您的文件加密特殊的驱动器。

当地位的按钮是绿色，安全的风险，您的系统是在最低限度。把绿色按钮，请执行下列步骤:

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

12.4. 漏洞扫描

可能影响漏洞检测的问题都以简单明了的描述列出，如果有影响您计算机安全的问题，在其后会显示一个红色的状态按钮 修复。 否则，将会心事一个绿色 确定 状态按钮

问题	说明
漏洞检测已启用	监控Windows更新、Office更新及Windows账户密码，以确保您的操作系统已经安装了最新补丁，同时密码不会被轻易攻破。
Microsoft关键更新	安装可用的Microsoft关键更新。
Microsoft其他更新	安装可用的Microsoft非关键更新。

问题	说明
Windows自动更新已启用	在新的Windows安全更新可用时第一时间安装它们。
管理员（强密码）	表明某个账户的密码强度。

如果状态按钮显示为绿色，则您系统的安全风险很小。要把按钮变为绿色，请执行以下步骤:

1. 点击 修复 按钮逐个修复安全漏洞。
2. 如果某个问题不能在此窗口解决，请按照向导的引导来修复它。

如果您想取消监控某个问题，请清除 监控 复选框。

13. 注册

BitDefender全方位安全杀毒软件有30天的试用期。 如果您想要注册bitdefender全方位安全杀毒软件.改变的授权码或创造一个新的bitdefender帐户，请点击 注册链接，位于底部的bitdefender窗口。 注册向导将会出现。

13.1. 步骤1/1 – 注册 Bitdefender全方位安全杀毒软件

BitDefender全方位安全杀毒软件2009

注册向导

请依照下方的指导注册您的 BitDefender 产品。

您当前的 BitDefender 授权状态为： 试用版

您当前的 BitDefender 授权密钥为： BE1B409B7E067AD03090

此授权密钥将过期于： 30 天

授权选项

如需继续使用当前密钥，请选择第一个选项。如需添加新的密钥，请选择第二个选项并填写密钥于下方的编辑框。

继续使用当前密钥

我想要使用新的密钥注册产品

输入新的授权密钥：

购买授权密钥

如需购买授权密钥，请点击下方的链接。

续订您的 BitDefender 授权密钥

您可在此找到您的授权密钥：

1) CD-Rom 标签

2) 产品注册卡

3) 在线购买邮件

bitdefender 完成 取消

注册

您可以看到Bitdefender注册状态，当前的授权密钥以及距离密钥过期所剩天数。

注册 Bitdefender 全方位安全杀毒软件

1. 选择我想要使用新的密钥注册产品。



2. 在编辑框中输入授权密钥。



注意

您可以找到您的授权密钥:

■在光盘标签上。

■在产品注册卡上。

■在网上购买的电子邮件中。

如果您没有Bitdefender授权密钥，请点击产品中所提供的链接前往Bitdefender网站购买。

点击完成。



14. 历史记录

点击位于BitDefender主窗口底部的 历史记录 链接会打开一个新窗口，其中显示BitDefender的历史记录及事件。这些信息让您可以概览安全相关的事件。 例如，您可以方便地检查升级是否成功执行、是否在计算机上发现恶意软件等。



事件

为了帮助您更好的筛选历史记录及事件，在左侧提供了下面的类别：

- ■反病毒
- ■防火墙
- ■反垃圾邮件
- ■隐私控制
- ■家长控制
- ■升级
- ■家庭网络

■文件库

可以查看每个类别的事件列表，每个事件都有如下信息：简述、事件发生时BitDefender采取的操作，以及事件发生的日期及时间。如果您想了解某个时间更多的鹅信息，请双击该事件。

如果想删除老日志，请点击 清除日志，如果希望最新日志显示出来，请点击 刷新。

高级管理

15. 常规

常规模块显示BitDefender活动信息及您计算机的系统信息。 您也可在此修改BitDefender的常规设置。

15.1. 图表板

要查看产品的活动统计信息和您的注册状态，请访问高级视图中的 常规>图表板。



图表板

图表板包含多个部分：

■统计 – 显示有关BitDefender活动的重要信息。

■概览 – 显示升级状态、您的账户状态、注册及密钥信息。



- 文件区域 – 显示BitDefender扫描的对象的变化情况，线条的高度表示在该时段内的扫描强度。
- 网络区域–BitDefender防火墙过滤了来自网络的流量。状态栏的高度表明了在这段时间间隔的流量。

15.1.1. 统计

如果您要关注的BitDefender活动，一个良好的开端是统计部分。 您可以看到以下项目：

项目	说明
已扫描的文件	表示上次扫描时所检测的文件总数。
已清除病毒文件	表示上次扫描时被清除病毒的文件总数。
检测到的病毒	表示上次扫描时发现的病毒总数。
阻止端口扫描	显示比特梵德防火墙端口扫描阻止的数据 端口扫描往往是黑客用来寻找计算机上的开放端口,用以利用它们。 保持 防火墙 及 静默模式 为启用状态以免受端口扫描侵害。

15.1.2. 概览

在这里您可以看到有关升级状态、您的账号状态、注册及授权密钥的信息。

项目	说明
上次升级	显示您上次升级Bitdefender产品的日期，请定期升级以确保系统得到有效防护。
我的账户	显示您的电子邮件地址，您可用此地址登录您的在线账户，找回您丢失的BitDefender授权密钥，并获取技术及客户服务。
注册	显示您的授权密钥类型和状态。为确保您的系统安全，在密钥过期后请及时更新密钥。
将到期于	显示授权密钥过期的剩余天数。

15.2. 设置

要配置BitDefender的常规设置，请到高级视图的 常规>设置 。



常规设定

在这里您可以设置BitDefender的整体行为。默认情况下，BitDefender在Windows启动时会被加载并最小化运行在任务栏中。

15.2.1. 常规设定

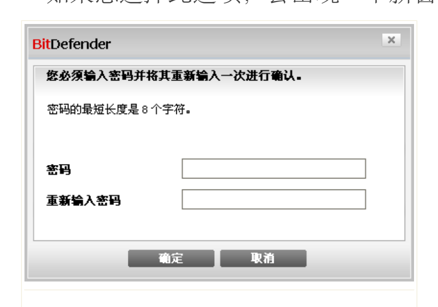
■为设置操作启用密码保护 － 设定一个密码，以保护BitDefender设置选项不被无权限的人修改。



注意

如果您不是使用这台电脑的唯一一个用户管理员权限的人，建议您为您的BitDefender配置项设置密码。

如果您选择此选项，会出现一个新窗口：



输入密码

在 密码 输入框输入密码，在 再次输入密码 输入框再输入一遍，然后点击 确定。

在您设置了密码之后，每当您要修改BitDefender设置选项时，都会要求您输入密码。 其他的系统管理员（如果有的话）也必须提供这个密码才能修改Bitdefender设置。

如果你想配置父母控制时被提示输入密码，你还必须选择 要求/申请家长控制专用密码. 在另一方面，如果一个密码才订定为父母控制和你选了这个选项，各自的密码将被要求配置的时候，任何bitdefender选择。



重要

如果您忘记了密码，您必须修复产品以修改BitDefender设置。

■要求有密码的时候，当我启动家长控制时,询问我是否设置一个密码 –当你启动了家长控制,同时还没有设定密码时,将会提示您设定密码 通过设置一个密码，你将阻止其他用户对行政权力运作，从改变父母控制设置你的配置，为特定的用户。

■显示BitDefender资讯（安全相关通知） – 不定期显示由BitDefender服务器发送的病毒爆发通知。

■在显示弹出消息（屏幕显示） – 显示产品状态相关的弹出窗口。 您可以配置BitDefender只在使用基本视图或高级视图显示弹出窗口。

■系统启动时加载BitDefender – 在系统启动时自动运行BitDefender。 建议选中这个选项。

■启用扫描活动工具栏（图形化显示的产品活动） – 在您登录Windows后显示 扫描活动条。 如果您不想显示扫描活动条，请清除此复选框。



注意
这个选项只可配置给当前Windows用户账户。

15.2.2. 病毒报告设置

■发送病毒报告 – 把在你的电脑发现的病毒报告给BitDefender病毒实验室，这将帮助我们了解和追踪病毒的爆发。

该报告将不会含有机密数据，例如您的名字、IP地址或其他资料，也不会用于商业目的。 资料将只包括病毒名称，且仅用作生成统计报告。

■启用病毒爆发报告 – 将潜在的病毒爆发报告发送给BitDefender实验室。

该报告将不会含有机密数据，例如您的名字、IP地址或其他信息，也不会用于商业目的。 资料将只包括可能的病毒，且仅用作检测新病毒。

15.3. 系统信息

您可以在此查看你计算机的所有的系统设置及自动运行程序，这样您可以监控计算机的状况，以及所安装的程序情况，从而发现可能的系统感染。

要获取系统信息，请到高级视图中的 常规>系统信息。



系统信息

列表包含所有在系统启动时自动加载的项目，以及有各个应用程序加载的项目。

有三个按钮可用：

■恢复 – 将当前的文件关联恢复到默认值。 仅适用 文件关联 设置!

■转到 – 打开一个窗口，显示所选的项目（例如 注册表）。



注意

根据所选项目的不同，转到 按钮不一定出现。

■刷新 – 重新打开 系统信息 部分。

16. 反病毒

Bitdefender保护您的电脑免受各类的恶意软件侵害（如病毒、木马、间谍软件、rootkit等）。 BitDefender病毒保护分为两类:

■实时防护 – 防止新的恶意软件威胁进入您的系统。 举例来说，Bitdefender会在您打开一个Word文档时扫描其中是否存在病毒，或者在您接受电子邮件时对其进行扫描。



注意
实时保护也被称为访问时扫描 – 文件在用户访问时被扫描。

■手动扫描 – 检测并清除系统中已经存在的恶意软件。 这是由用户启动的传统扫描方式 – 用户选择要扫描的磁盘、文件夹，BitDefender按照用户的需求进行扫描。 扫描任务让您能够创建自定义的扫描例行作业，并可设置为按照计划定期执行。

16.1. 实时防护

BitDefender扫描所有被访问的文件、电子邮件消息和即时通讯流量，为您提供连续的实时防护，保证系统远离恶意软件。 BitDefender反钓鱼功能在您上网时提醒您可能存在钓鱼风险的网页，从而保护您的个人信息不被泄露。

要配置实时防护和BitDefender反钓鱼功能，请到高级视图中的 反病毒>实时防护。



实时防护

您可以查看实时防护是启用还是禁用。 如果您想更改实时防护状态，请清除或选中对应的复选框。



重要

为防止病毒感染您的计算机，请保持启用 实时防护。

要启动快速系统扫描，请点击 立即扫描。

16.1.1. 设置防护级别

您可以选择最符合您的防护需求的安全级别，上下拖动滚动条以设定最合适的防护级别。

共有3个防护级别:

防护级别	说明
宽松	覆盖基本安全需求，系统资源占用很低。 只扫描程序和邮件信息中的病毒。除了传统的基于特征码的扫描，还使用了启发式分析。对感染文件采取的措施为：清除文件/禁止访问。
默认	提供标准安全级别，资源消耗级别较低。 扫描所有文件和邮件信息中的病毒和间谍软件。除了传统的基于特征码的扫描，还使用了启发式分析。对感染文件采取的措施为：清除文件/禁止访问。
严格	提供高级安全级别，资源消耗级别中等。 扫描所有文件、邮件信息和网页流量中的病毒和间谍软件。除了传统的基于特征码扫描之外，还使用了启发式分析。对感染文件采取的措施为：清除文件/禁止访问。

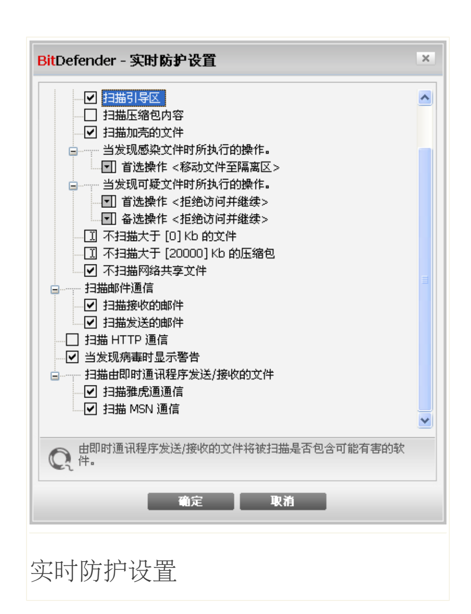
要启用默认的实时防护设置，请点击 默认级别。

16.1.2. 自定义级别

高级用户可以使用BitDefender提供的扫描设置功能，可以在这里设置扫描程序只扫描特定文件扩展名、查找特定恶意软件类型或者跳过压缩文档。这将可以极大降低扫描时间，并提升您计算机在扫描过程中的响应速度。

要自定义 实时防护，请点击自定义级别，下面的窗口会出现：





实时防护设置

扫描选项以可扩展菜单的形式展现，和Windows中的类似。 按"+"的可以展开选项，按 “–” 收起选项。



注意

您会发现有些选项虽然有 “+” 号却无法展开，这是因为这些选项尚未被选中，如果您选中它们，就可以展开了。

■扫描访问的文件及即时通讯流量 – 扫描被访问的文件，以及通过即时通讯工具的通信（QQ、雅虎通、MSN等） 。此外，请选择您想扫描的文件类型。

选项		说明
扫描访问的文件	扫描所有文件	扫描所有被访问的文件，无论是何种类型。
	只扫描程序文件	只扫描带有下列扩展名的程序文件: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta;

选项		说明
		.html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws。
	只扫描用户指定的文件扩展名	只扫描带有用户指定的文件扩展名的文件，请用“;”分隔各个文件扩展名。
	扫描风险软件	扫描风险软件。 检测到的文件将被作为感染文件处理，启用此选项后，包含广告软件组件的软件可能会停止运行。 如果你想排除拨号程序和应用程序的话，请选择跳过拨号软件和应用软件扫描。
扫描引导扇区		扫描系统的引导扇区。
扫描压缩包内容		扫描被访问的压缩文档，启用此选项后，计算机速度会变慢。
扫描加壳文件		所有的加壳文件将会被扫描。
首选操作		请从下拉菜单中选择针对感染文件和可以文件的首选操作：
	拒绝访问并继续	如果发现感染的文件，会阻止对该文件的访问。
	清除文件	清除受感染的文件。
	删除文件	没有任何警告下立即删除受感染的文件。
	移动文件至隔离区	受感染的文件移到隔离区。
备选操作		请从下拉菜单中选择针对感染文件备选操作，当首选操作失败后会进行备选操作。
	拒绝访问并继续	如果发现感染的文件，会阻止对该文件的访问。
	删除文件	没有任何警告下立即删除受感染的文件。
	移动文件至隔离区	受感染的文件移到隔离区。
不扫描大于[x]Kb的文件。		输入要扫描的文件的最大尺寸，如果设置为0Kb，则所有文件都会被扫描。

选项	说明
不扫描大于[20000]KB的压缩文件	输入希望扫描的压缩文件的最大尺寸（ KB）。 如果您想扫描所有压缩文件，而不论其大小，请输入0。
不扫描共享文件夹	如果启用了此选项，Bitdefender将不会扫描网络共享文件夹，避免影响网络速度。 如果您所在的网络已经有反病毒解决方案，建议您启用此选项。

■扫描电子邮件通信 – 扫描电子邮件通信。

您可选择以下任务:

选项	说明
扫描接收的邮件	扫描所有接收到的邮件信息。
扫描发出的邮件	扫描所有发出邮件信息。

■扫描HTTP通信
■发现病毒时显示警告 – 当在文件或电子邮件中发现病毒是显示警告窗口。

如果是被感染文件，警告窗口会包含病毒名称、文件路径、BitDefender所采取的操作，以及一个指向BitDefender网站更多信息的链接。如果是被感染的电子邮件，警告窗口还会包含发件人和收件人信息。

如果发现的是可疑文件，您可以从警告窗口打开一个向导，该向导会帮助您将可疑文件发送到BitDefender实验室做进一步分析。您可以输入您的电子邮件地址以便接收有关此文件的信息。
■扫描由即时通讯程序接收/发送的文件. 如要扫描您通过雅虎通或MSN收发的文件，请选中此选项。

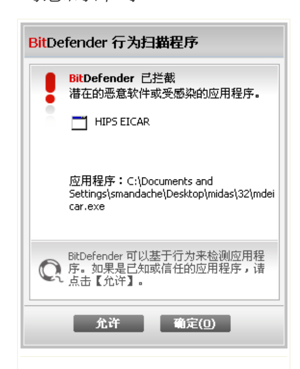
点击 确定 保存修改并关闭窗口。

16.1.3. 设置行为扫描程序

行为扫描程序提供对还没有特征码的新病毒的防护。 它持续地监测和分析您计算机上运行的应用程序的行为，如果发现某个应用程序有可疑行为，就会向您发出警告。



每当一个应用程序试图执行可能的恶意操作时，行为扫描程序就会发出警告，并征询您的许可。

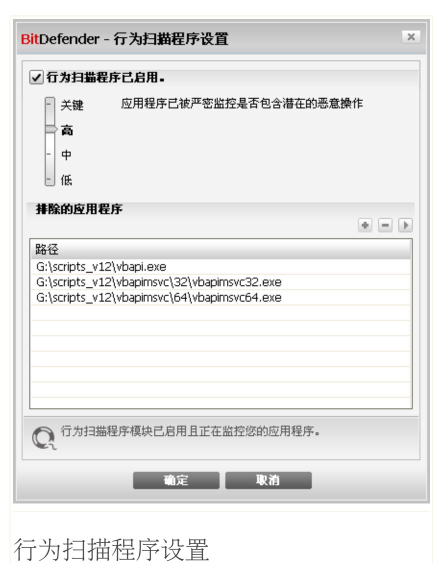


行为扫描程序报警

如果您了解并信任所检测到的应用程序，请点击 允许。行为扫描程序将不再扫描该应用程序的恶意行为。

如果您想立即关闭该应用程序，请点击确定。

要设置行为扫描程序，请点击 扫描程序设置。



行为扫描程序设置

如果您想禁用行为扫描程序，请清除 行为扫描仪已启用 复选框。



重要
保持启用行为扫描程序，才能免受未知病毒侵害。

设置防护级别

当您设置了新的实时防护级别时，行为扫描程序的防护级别会随之自动改变。 如果您不满意默认设置，您可以手动配置防护级别。



注意
请记住，如果您改变了当前的实时防护级别，行为扫描程序的防护级别也会相应改变。

请拖动滚动条选择最适合您需求的防护级别。

防护级别	说明
关键	严格监控应用程序可能的恶意操作。
高	高强度监测应用程序可能的恶意操作。
中	中等强度监测应用程序可能的恶意操作。
低	监测应用程序可能的恶意操作。

管理排除的应用程序

您可以设置行为扫描程序不扫描特定的应用程序。 当前未被行为扫描程序扫描的应用程序显示在 排除的应用程序 表中。

要管理排除的应用程序，您可以使用位于表格上方的按钮:

- Add - exclude a new application from scanning.
- Remove - remove an application from the list.
- Edit - edit an application path.

16.1.4. 禁用实时防护

如果您想禁用实时防护，会显示一个警告窗口。



禁用实时防护

您需要从列表中选择您想禁用实时防护多长时间，以确认您的选择。您可选择禁用实时防护5分钟、15分钟、30分钟、1小时或者禁止到下次系统重启。



警告
这是个非常关键的安全问题，建议您禁用实时防护的时间尽量短。如果实时防护被禁止，您将不再被保护免遭恶意软件威胁。

16.1.5. 设置反钓鱼防护

BitDefender为下列软件提供实时反钓鱼防护：

- Internet Explorer
- Mozilla Firefox
- 雅虎通
- MSN

您可选择完全禁止反钓鱼防护或者只针对特定应用禁止。

您可以点击白名单来设置管理一个不需要被BitDefender反钓鱼引擎扫描的网站列表。



BitDefender - Antiphishing

白名单

此列表中的URL不会被BitDefender扫描。

白名单中的网址将不会被BitDefender反钓鱼引擎检查。BitDefender将不会通知您这些网页中的威胁。

新建地址 添加

网站

www.google.ro 移除

点击此处可添加地址至反钓鱼白名单。

保存 关闭

反钓鱼白名单

您可以看到当前BitDefender不进行钓鱼风险扫描的网站列表。

要向白名单中添加新的网站，请在新建地址 输入网址并按 添加。 白名单应只包含您完全信任的网站。 例如，添加您经常上的购物网站。



注意

您可以方便地从集成到浏览器上的BitDefender反钓鱼工具栏添加网站到白名单。

如果要从白名单中删除一个网站，请点击 移除按钮。

点击 关闭 保存更改并关闭窗口。

16.2. 手动扫描

BitDefender的首要任务是保证您的计算机干净无毒，因此产品会阻止新病毒进入您的计算机，并扫描所有电子邮件、新下载文件及新复制的文件。

但是病毒可能在安装BitDefender之前就已经存在于您的计算机中，因此在安装BitDefender之后最好扫描一次您的计算机，当然如果能定期扫描就会更安全。

要配置并启动手动扫描，请到高级视图中的 反病毒>病毒扫描。

扫描任务

手动扫描基于系统扫描任务，扫描任务指定扫描的选项以及需要扫描的对象。 您可以随时运行默认的扫描任务或者您自定义的扫描任务扫描您的计算机，您还可为扫描任务设置运行计划，以便定时运行扫描任务或者在系统空闲时运行。

16.2.1. 扫描任务

BitDefender已经默认定义了几个扫描任务，这些任务覆盖了常见的安全问题，您也可以创建并设置自定义的扫描任务。

每个扫描任务都有一个属性 窗口，您可在其中配置扫描任务并查看扫描结果。欲了解更多信息，请参阅 “设置扫描任务” （第 134 页）。

扫描任务可分为三种：

■系统扫描任务 – 包含以下默认的系统扫描任务：

系统扫描任务	说明
深度系统扫描	扫描整个系统，包括压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。
全面系统扫描	扫描整个计算机，不扫描压缩文档。 在默认配置下，它扫描所有威胁您系统安全的恶意软件，如病毒、间谍软件、广告软件、rootkit等。
快速系统扫描	扫描 Windows ， Program Files 和 All Users 文件夹。 在默认配置下，扫描除rootkit之外的所有类型恶意软件，但不扫描内存、注册表和Cookie。
自动登录扫描	扫描当用户登录到Windows操作系统时被运行的项目。 默认情况下， 自动登录扫描被禁用。 如果您想使用这项任务，请用右键点击它，选择 任务计划 并设置任务在 系统启动时运行。 您可以指定在系统启动后多长时间运行此扫描任务。



注意

由于深系统度扫描和全面系统扫描任务分析整个系统，扫描可能需要占用较长时间。因此，我们建议您用较低优先级运行这些任务，或在系统处于闲置状态是运行这些任务。

■用户扫描任务 包含用户自定义的扫描任务。

默认提供了一个名为 扫描我的文档的任务。 使用这项任务扫描当前用户的重要文件夹：我的文档，桌面　 和 启动 。这会确保您的文档和工作环境安全，并保证系统启动时运行的应用程序是安全的。

■其他扫描任务　 －包含多个其他扫描任务，这些任务比较独特，不能从本窗口启动。您只能修改这些任务的设置，或查看扫描报告。

在每个任务的右侧有三个按钮：

■ 任务计划 － 表示此扫描任务已被设置为稍后运行。点击此按钮可打开　属性窗口的 任务计划 标签，您在在此标签页中查看该任务的运行计划并进行修改。

■ 删除 － 删除所选任务。



注意

对系统扫描任务无效。用户无法删除系统任务。

■ 立即扫描 – 运行扫描任务，启动 即时扫描。

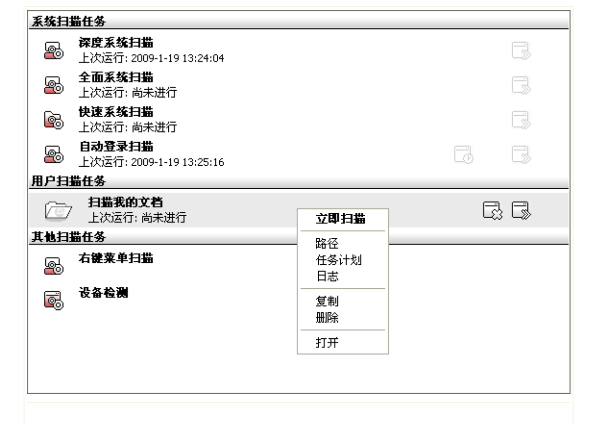
在每项任务的左边，您可看到 属性 按钮，您可点击此按钮进入属性窗口设置该任务，并可查看扫描日志。

16.2.2. 使用快捷菜单

每个扫描任务都有快捷菜单，在任务上单击鼠标右键就可打开快捷菜单。

快捷菜单上包含以下命令：

立即扫描 – 运行选定的扫描任务，启用即时扫描。



快捷菜单



■路径 – 打开 属性 窗口的 路径 标签页，您可在此修改选定任务的扫描对象。



注意

如果是系统扫描任务，此选项会被替换为 显示任务路径，因为您只能查看系统任务的扫描对象而不能修改。

■任务计划 – 打开 属性 窗口的 任务计划 标签页，您可在此为选定的任务设置运行计划。

■日志 – 打开属性 窗口的 日志 标签页，您可在此查看选定任务运行后生成的扫描报告。

- 复制 – 复制指定的扫描任务。 这在建立新任务时非常有用，因为您可通过复制并修改已有的扫描任务快速创建一个新任务。
- 删除 – 删除指定的扫描任务。

注意
对系统扫描任务无效。用户无法删除系统任务。

- 打开 – 打开 属性 窗口的 概览 标签页，您可在此修改所选任务的选项。

注意
由于 其他扫描任务 的特殊性，其快捷菜单只包含 属性 和 日志 两个命令。

16.2.3. 创建扫描任务

您可通过如下方法来创建扫描任务：

- 复制 一个现有任务并重新命名，然后在 属性 窗口进行必要的修改。
- 点击 新建任务 创建一个新任务并进行配置。

16.2.4. 设置扫描任务

每个扫描任务都有 属性 窗口，用户可以设置扫描选项、扫描对象、计划任务或查看扫描日志。 要打开属性窗口，请点击任务右侧的 打开 按钮，或者右键点击任务并点击快捷菜单中的 打开。



注意
欲了解更多有关在 日志 标签页中查看扫描日志的信息，请参阅 "查看扫描日志"(第 151 页)。

设置扫描选项

要为某个扫描任务设置扫描选项，请右键点击该任务，并选择 属性。 就会出现下面的窗口：



概览

您可在此查看该任务的信息（名称、上次运行时间及任务计划状态），并设置扫描选项。

选择扫描级别

您可通过选择一个扫描级别轻松配置扫描选项，请拖动滚动条选择合适的扫描级别。

共有三个扫描级别:

防护级别	说明
低	提供合理的检测效率，资源消耗水平低。 只扫描程序中的病毒。除了经典的特征码病毒扫描外，还使用了启发式分析。
中	提供良好的检测效率，中等资源消耗水平。 扫描所有文件中的病毒和间谍软件。除了经典的特征码病毒扫描外，还使用了启发式分析。
高	提供极高的检测效率，资源消耗水平很高。

防护级别	说明
	扫描所有文件和压缩文档中的病毒和间谍软件。除了经典的特征码病毒扫描外，还使用了启发式分析。

还有下列适用于扫描进程的常规选项：

- 以低优先级运行任务. 调低扫描过程的优先级，这将让其他程序运行速度更快，并增加扫描进程完成的时间。
- 扫描窗口启动时最小化至托盘. 将扫描窗口最小化到 系统托盘，双击BitDefender系统托盘图标可以打开窗口。
- 当扫描完成且未发现威胁时关闭计算机

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

自定义扫描级别

高级用户可以使用BitDefender提供的扫描设置功能，可以在这里设置扫描程序只扫描特定文件扩展名、查找特定恶意软件类型或者跳过压缩文档。这将可以极大降低扫描时间，并提升您计算机在扫描过程中的响应速度。

点击 自定义设置您自己的扫描选项，一个新窗口会出现。





扫描级别设置

扫描选项以可扩展菜单的形式展现，和Windows中的类似。 按"+"的可以展开选项，按 “–” 收起选项。

扫描选项分为三个类别：

■扫描级别. 指定您希望BitDefender扫描的恶意软件类型，可通过从 扫描级别 分类中选择合适的选项完成。

选项	说明
扫描病毒	扫描已知的病毒。 BitDefender可以检测不完整的病毒体，因此可以清除任何威胁您的系统安全的恶意软件。
扫描广告软件	扫描广告软件，检测到的文件将被作为感染文件处理。如果启用此选项，包含广告组件的软件可能会停止工作。
扫描间谍软件	扫描已知间谍软件的威胁。检测出的文件将会被作为感染文件处理。

选项	说明
扫描应用程序	扫描可能被用作间谍工具、隐藏恶意应用程序或有其他恶意企图的合法应用程序。
扫描拨号器	扫描拨打高额花费电话号码的应用程序。检测到的文件将被作为感染文件处理，如果启用此选项，包含拨号器组件的软件可能会停止工作。
扫描rootkit	扫描隐藏对象（文件及进程），通常被称为rootkit。

■病毒扫描选项. 指定要扫描的对象类型（文件类型、压缩文件等），可从 病毒扫描选项 类别下选择合适的选项。

选项		说明
扫描文件	扫描所有文件	扫描所有文件，无论其是什么类型。
	只扫描程序文件	进扫描带有下述文件扩展名的程序文件：exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml and nws.
	只扫描用户指定的文件扩展名	只扫描带有用户指定的文件扩展名的文件，请用 “;” 分隔各个文件扩展名。
打开加壳程序		扫描加壳文件。
打开压缩包		扫描压缩包内部的文件。 扫描压缩文档会增加扫描时间，并会占用更多的系统资源。 您可点击压缩包大小限制 并输入要扫描的压缩包的最大值（ KB ）。
打开邮件档案		扫描邮件档案内部。
扫描引导扇区		扫描系统的引导扇区。
扫描内存		扫描内存以发现病毒和其他恶意软件。

选项	说明
扫描注册表	扫描注册表。
扫描Cookie	扫描Cookie文件。

■操作选项. 使用 操作选项 类别中的选项指定对所检测到的各种文件的操作。



注意
要设置一个新操作，请点击当前的操作并从下拉列表中选择。

· 选择对检测到的感染文件所采取的操作。 您可选择以下任务:

操作	说明
无需采取操作	不对受感染的文件采取任何操作，这些文件将被记录在扫描报告中。
清除病毒	删除被感染文件中的恶意代码。
删除文件	没有任何警告下立即删除受感染的文件。
移至隔离区	受感染的文件移到隔离区。 被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。

· 选择对检测到的可疑文件所采取的操作。 您可选择以下任务:

操作	说明
无需采取操作	不对可疑文件做任何操作，这些文件将会被记录在扫描报告中。
删除文件	直接删除可疑文件，不进行任何提示。
移至隔离区	移动可疑文件到隔离区。 被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。



注意
可疑文件是由启发式分析程序检测出来的，我们建议您将这些可疑文件发送给BitDefender实验室。

· 选择对所检测到的隐藏对象（Rootkit）所采取的操作。 您可选择以下任务:

操作	说明
无需采取操作	不对隐藏文件采取任何操作，这些文件将会被记录在扫描报告中。
移至隔离区	移动隐藏文件到隔离区。 被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。
重命名文件	给文件加上.bd.ren后缀，并使其属性为可见。

• 压缩文档操作选项. 扫描和处理压缩包内部的文件会受到一些限制。 有密码保护的档案不能被扫描，除非您提供密码。 根据压缩包格式的不同，BitDefender 可能无法清除、隔离或删除受感染的压缩包文件。 请从 压缩文档操作选项 类别选择针对检测到的压缩文件的合适操作选项。

◯选择对检测到的感染文件所采取的操作。 您可选择以下任务:

操作	说明
无需采取操作	仅在扫描日志中记录受感染的压缩文档信息。在扫描完成后，您可以打开扫描日志查看这些压缩文档的信息。
清除病毒	删除被感染文件中的恶意代码。 病毒清除操作在某些情况下可能会失败，比如清除在电子邮件档案内部的感染文件时。
删除文件	立即从磁盘删除受感染的文件，不做任何警告。
移至隔离区	移动受感染的文件从原来的位置移动到 隔离区。被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。

◯选择对检测到的可疑文件所采取的操作。 您可选择以下任务:

操作	说明
无需采取操作	只在扫描日志中记录可疑压缩文档的信息。 在扫描完成后，您可以打开扫描日志查看这些压缩文档的信息。
删除文件	直接删除可疑文件，不进行任何提示。

操作	说明
移至隔离区	移动可疑文件到隔离区。 被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。

○选择对检测到的受密码保护文件的操作选项。 您可选择以下任务:

操作	说明
记录为未扫描	只在扫描日志中记录受密码保护的文件的信息。在扫描完成后，您可以打开扫描日志查看这些压缩文档的信息。
提示输入密码	当一个密码保护的文件被检测到时，提示用户输入密码以扫描文件。



注意
如果您选择忽略检测到的文件，或者所选的操作失败，则您必须在扫描向导中选择一个操作。

点击 默认 可载入默认设置选项。 点击 确定 保存修改并关闭窗口。

设置扫描对象

要为某个用户扫描任务指定扫描对象，请右键点击 路径。 就会出现下面的窗口：



扫描对象

您可看到本地、网络及可移动硬盘，以及之前添加的文件或文件夹列表。所有被选中的项目将会在任务运行时被扫描。

本部分包含以下按钮:

■添加项目 – 打开一个窗口浏览并选择您想扫描的文件及文件夹。



注意
您也可以使用拖放功能向列表中添加文件/文件夹。

■删除项目 – 删除列表中之前添加的文件/文件夹。



注意
只能删除后来添加的文件/文件夹，BitDefender自动“发现”的对象不能被删除。

除了上面说明的按钮之外，还有一些其他选项可以帮您快速选择扫描对象。

■本地驱动器 – 扫描本地驱动器。



■网络驱动器 – 扫描所有的网络驱动器。
■可移动驱动器 – 扫描可移动驱动器 (光盘、软盘、U盘等)。
■所有项目 – 扫描所有驱动器, 无论是本地、网络或可移动驱动器。



注意
如果您想扫描整个计算机, 请选择对应 所有项目 的复选框。

点击 确定 保存更改并关闭窗口。要运行任务, 请点击 扫描。

查看系统扫描任务的扫描对象

您不能修改 系统扫描任务 中的扫描对象。 您只能查看系统扫描任务的扫描对象。

要查看某个系统扫描任务的扫描对象, 请右键点击该任务, 并选择 显示任务路径。以全面系统扫描 为例, 将会显示下面的窗口:



全面系统扫描的扫描对象

全面系统扫描 和 深度系统扫描 会扫描扫有的本地驱动器, 而 快速系统扫描 只扫描 Windows 和 Program Files 文件夹。

点击 确定 关闭窗口。 要运行任务, 请点击 扫描。

设置扫描任务运行计划

对于复杂的任务，扫描过程将持续较长时间，并且在您关闭其他程序时会运行得更好。因此最好为这些任务设置运行计划，在您不使用计算机或计算机空闲时运行这些任务。

要查看一个扫描任务的运行计划或对其进行修改，请右键点击该任务并选择 任务计划。 就会出现下面的窗口：



任务计划

您将看到已设定的任务计划。

在设置任务的运行计划时，您需要选择下列选项之一：

■没有计划 – 仅在用户请求时启动任务。

■一次 – 仅在特定时间运行该任务一次。指请在 开始日期/开始时间 设置开始运行的日期和时间。

■周期性 – 从某个特定日期开始，定时周期性运行该扫描任务（每小时、每天、每周、每月或每年）。



如果您希望扫描任务每隔一定时间周期性运行，请选择 周期性 并在 每隔 编辑框输入分钟数/小时/天/周/月/年，指定扫描的频率。您还需要在 开始日期/开始时间 里输入开始的日期和时间。

■于系统启动时 - 在用户登录Windows后的指定时间内启动扫描任务。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

16.2.5. 扫描对象

在您运行扫描任务之前。请确保Bitdefender已升级到最新的病毒库。用过时的病毒库扫描您的计算机可能会漏掉最新的恶意软件。要了解上次升级的时间，请在高级视图中点击 升级>升级。



注意

为了能让BitDefender进行完整扫描，您必须关闭所有运行的程序，尤其是您的电子邮件客户端（如如Outlook、Outlook Express 或 Foxmail等）。

扫描方式

BitDefender提供四种手动扫描方式

■即时扫描 - 从系统扫描任务或用户扫描任务中运行一个任务。
■右键菜单扫描 - 右键点击一个文件或文件夹并启用BitDefender反病毒2009.
■拖放扫描 - 拖放文件或文件夹 到 扫描活动条。
■手动扫描 - 使用Bitdefender手动扫描，直接选取要扫描的文件或文件夹。

即时扫描

要全部或部分扫描您的计算机，您可运行默认的扫描任务或您自己创建的任务。 这被称作即时扫描。

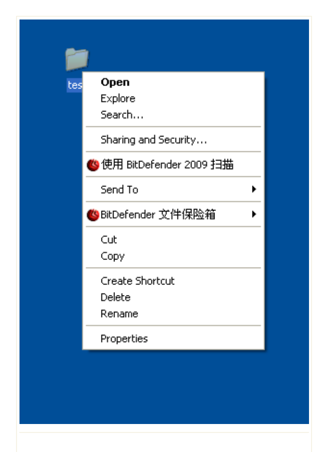
要运行一个任务，请采用下述方法之一:

■在列表中双击希望运行的扫描任务。
■点击对应此任务的 立刻扫描 按钮。
■选择该任务并点击 运行任务。

Bitdefender扫描程序将会显示并启动扫描过程。 欲了解更多信息，请参阅 “BitDefender扫描程序” (第 147 页)。

右键菜单扫描

如果想不创建扫描任务就扫描一个文件或文件夹，您可以使用右键菜单扫描。 这被称为右键菜单扫描。



右键菜单扫描

右键点击您想扫描的文件或文件夹，然后选择 使用 BitDefender 2009扫描。

Bitdefender扫描程序将会显示并启动扫描过程。 欲了解更多信息，请参阅 “BitDefender扫描程序” (第 147 页)。

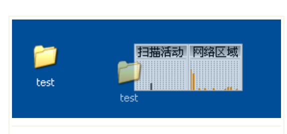
您可通过 右键菜单扫描 任务的 属性 窗口查看扫描报告，或修改扫描选项。

拖放扫描

拖动您想扫描的文件或文件夹，将其放到 扫描活动条上，如下图所示。



拖放扫描



放下文件

Bitdefender扫描程序将会显示并启动扫描过程。 欲了解更多信息，请参阅“BitDefender扫描程序”（第 147 页）。

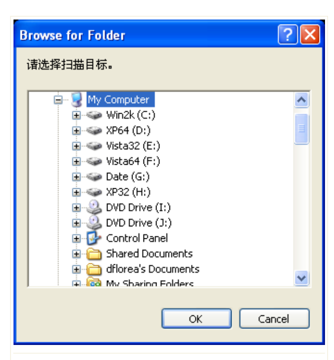
手工扫描

手工扫描需要从BitDefender的程序组中选择手工扫描程序，然后直接指定要扫描的对象。



注意
手动扫描非常有用，因为它可以运行在Windows的安全模式下。

要选择BitDefender的扫描对象，请从Windows开始菜单上，按以下顺序点击：开始 → 程序 → Bitdefender 2009 → Bitdefender手工扫描。 就会出现下面的窗口：



手工扫描

选择您想扫描的对象并点击 确定。

Bitdefender扫描程序将会显示并启动扫描过程。 欲了解更多信息，请参阅 “BitDefender扫描程序”（第 147 页）。

BitDefender扫描程序

当您启动一个手动扫描进程后，BitDefender扫描程序就会出现。 请遵循向导程序的三个步骤来完成扫描过程。

步骤 1/3 — 正在扫描

Bitdefender将开始扫描选定的对象。





正在扫描

您可以看到扫描的状态和统计信息（扫描速度、已用时间、扫描/感染/可疑/隐藏对象的数目等）。



注意

扫描过程可能需要较长时间，取决于扫描的复杂程度。

要暂停扫描进程，请点击 暂停。之后可以点击 继续 继续扫描。

您可以在任何时候点击 停止&确认停止扫描，停止后您将进入扫描向导的最后一个步骤。

请等待Bitdefender完成扫描。

步骤 2/3 — 选择操作

当扫描完成后，将会出现一个新窗口，您可在此窗口看到扫描结果。



选择操作

您可看到影响您计算机的问题数。

被感染的对象根据它们所感染的病毒分组显示。 点击对应某个病毒的链接，可以看到感染对象的更多信息。

您可以为所有的文件选择一个统一的操作，也可单独为每组文件单独选择操作。

您可选择以下操作:

操作	说明
不采取任何操作	对检测出的文件不做任何操作。
清除病毒	清除受感染的文件。
删除文件	删除检测出的文件。
移动至隔离区	将检测出的文件移动到隔离区。

点击 继续 执行所选的操作。

步骤 3/3 — 查看结果

当BitDefender完成处理检测出的问题后，将会在一个新窗口显示扫描结果。



扫描结果摘要

您可看到扫描结果的摘要。 点击查看日志 查看扫描日志。



重要

如有需要，请重新启动系统以完成清除过程。

点击 关闭 关闭窗口。

Bitdefender未能解决部分问题

在大多数情况下，Bitdefender能成功清除受感染的文件或隔离受感染的文件。 但是，有些问题当时不能得到解决。

如果您遇到这种情况，请联系Bitdefender支持团队www.bitdefender.com。 我们的技术支持人员将帮助您解决问题。

Bitdefender检测到可疑文件

可疑文件是被启发式分析程序检测为可能感染了未知的病毒特征码。

如果在扫描中检测到了可疑文件，您将被请求发送这些文件给BitDefender实验室。点击 确认 发送这些文件给Bitdefender实验室进行分析。

16.2.6. 查看扫描日志

要查看扫描任务运行完之后的扫描日志，请右键点击该任务并选择 日志。 就会出现下面的窗口：



查看扫描日志

您可在此查看每次扫描任务被运行后生成的日志文件。 每个文件中都会显示扫描过程的状态信息，扫描的日期和时间，以及扫描结果摘要。

有两个可用按钮：

■删除 – 删除选定的扫描日志。
■打开 – 打开并查看选定的扫描日志。 扫描日志会在默认浏览器中打开。





注意
此外，要查看或删除一个日志文件，可以右键点击该文件然后从右键菜单中选择对应的选项。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

扫描日志示例

下图是扫描日志的一个示例：



扫描日志示例

扫描日志包含扫描过程的详细信息，如扫描选项、扫描对象、发现的病毒，以及针对各个文件采取的操作等。

16.3. 不进行扫描的对象（白名单）

有时不希望扫描特定的文件，比如您可能不想EICAR测试文件被实时防护扫描程序扫描，或者不希望 .AVI 文件被手动扫描任务扫描。

BitDefender可以在实时防护、手动扫描或两者中排除对指定对象的扫描。这个功能是为了减少扫描时间，并避免影响您的工作。

有两种类型的对象可以被排除扫描：

- 路径 – 由一个路径表示的文件或文件夹（包括其中的所有对象）将会被扫描程序排除扫描。
- 文件扩展名 – 所有带有指定文件扩展名的文件将会被排除扫描。



注意

被排除于实时防护扫描的对象，无论是被您或应用程序访问时都不会被扫描。

要查看和管理排除扫描的对象，请到高级视图中的 反病毒>白名单。

BitDefender 全方位安全杀毒软件 - 试用版　切换至基本视图

状态：5 个等待处理的问题　修复

实时防护 | 病毒扫描 | 白名单 | 隔离区

常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册

☑ 白名单已启用

不会被扫描的对象	实时防护	手动扫描
文件及目录		
c:\	是	是
文件扩展名		
*.zip (压缩包)	是	是

应用　丢弃

点击此处可应用最近更改

bitdefender　购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

扫描白名单

您可以看到被排除扫描的对象（文件、文件夹及文件扩展名），对于每个对象，您能看到它是被排除于实时防护、手动扫描还是两者都排除。



注意

此处指定的白名单不会影响右键菜单扫描。

要从列表中删除一个对象，请选择它然后点击 ▭ 删除 按钮。

要修改一个条目，请选中它并点击 ▷ 编辑 按钮。 将会出现一个新窗口，您可在其中修改要排除的文件扩展名或路径击，并输入您想应用此排除的扫描类型。修改后请点击 确定。



注意

您也可以右键点击一个对象，并使用快捷菜单上的选项进行编辑或删除。

您可以点击 丢弃 恢复对规则表所做的修改，只要还没有点击 应用保存修改。

16.3.1. 排除扫描的路径

要排除扫描路径，请点击 添加 按钮。 将会显示配置向导，引导您完成设置要排除扫描的路径。

步骤 1/4 – 选择对象类型



选择对象类型

选择 “不扫描文件或路径” 。

点击 下一步。

步骤 2/4 - 指定要排除的路径

BitDefender全方位安全杀毒软件2009

扫描白名单向导 - 步骤 2 / 4

步骤 1 步骤 2 步骤 3 步骤 4

白名单路径

请在此输入不需要被扫描的路径

浏览 添加

选定的路径

c:\

您可在上方浏览不会被扫描的路径。选择路径（文件或目录）后请务必点击【添加】按钮。您可添加多个项目至此列表。

请仔细为扫描过程选择白名单。请注意，建议您不定义任何白名单，以确保您的系统受到完全的保护。

bitdefender 上一步 下一步 取消

排除的路径

要指定排除扫描的路径，请使用下述方法之一：

■点击 浏览，然后选择要被排除的文件或路径，接着点击 添加。
■在编辑框中输入您想排除的路径，然后点击 添加。



注意

如果提供的路径并不存在，将会显示错误信息。点击确定 并检查路径是否有效。

路径将出现在列表中，您可添加任意多的路径。

要从列表中删除一个对象，请选择它然后点击 ▭ 删除 按钮。

点击 下一步。

步骤 3/4 - 选择扫描类型

BitDefender全方位安全杀毒软件2009

扫描白名单向导 - 步骤 3 / 4

步骤 1 步骤 2 步骤 3 步骤 4

何时应用

请选择将被应用至选定白名单条目的扫描类型：手动扫描、实时防护，或两者都选。请点击右侧表格栏列中的单元格文本并按需选择您的选项。

选定的对象	何时应用
c:\	两者

请仔细为扫描过程选择白名单。请注意，建议您不定义任何白名单，以确保您的系统受到完全的保护。

bitdefender 上一步 下一步 取消

扫描类型

您可看到被排除于扫描的路径列表，以及它们被排除于何种扫描类型。

默认情况下，选定的路径被排除在实时防护和手动扫描。要更改何时应用排除规则，请点击右边的栏并选择你希望的选项。

点击 下一步。



步骤 4/4 – 扫描排除的文件



扫描排除的文件

强烈建议您在把路径添加到白名单列表之前对它们进行扫描，以确保它们是干净无毒的。 选中复选框以便在添加到白名单之前扫描这些文件。

点击完成。

点击 应用 保存修改。

16.3.2. 排除扫描文件扩展名

要排除扫描文件扩展名，请点击 添加 按钮。 随后出现的配置向导会引导您完成设置要排除的文件扩展名。

步骤 1/4 – 选择对象类型



选择对象类型

选择“不扫描文件扩展名”。

点击 下一步。

步骤 2/4 - 指定要排除的文件扩展名

BitDefender全方位安全杀毒软件2009

扫描白名单向导 - 步骤 2 / 4

步骤 1 步骤 2 步骤 3 步骤 4

BitDefender扫描白名单向导

请在此输入不需要被扫描的扩展名

zip 添加

.zip (压缩包) 将不会被扫描

选定的扩展名

您可在上方选择不会被扫描的扩展名。选择某扩展名后请点击【添加】按钮。您可添加多个项目至此列表。

请仔细为扫描过程选择白名单。请注意，建议您不定义任何白名单，以确保您的系统受到完全的保护。

bitdefender 上一步 下一步 取消

排除的文件扩展名

要指定排除的文件扩展名，请采用下述方法之一：

■从下拉列表中选择您想排除的文件扩展名，并点击 添加。



注意

下拉列表中包含了您计算机上登记的所有文件扩展名，当您选中一个文件扩展名时，如果有其描述，则会显示出来。

■在编辑框中输入您想排除的文件扩展名并点击 添加。

文件扩展名将出现在表中，您可添加任意多的文件扩展名。

要从列表中删除一个对象，请选择它然后点击 ▭ 删除 按钮。

点击 下一步。

步骤 3/4 - 选择扫描类型

BitDefender全方位安全杀毒软件2009

扫描白名单向导 - 步骤 3 / 4

步骤 1 步骤 2 步骤 3 步骤 4

何时应用

请选择将被应用至选定白名单条目的扫描类型：手动扫描、实时防护，或两者都选。请点击右侧表格栏列中的单元格文本并按需选择您的选项。

选定的对象	何时应用
*.zip (压缩包)	两者

请仔细为扫描过程选择白名单。请注意，建议您不定义任何白名单，以确保您的系统受到完全的保护。

bitdefender 上一步 下一步 取消

扫描类型

您可看到包含被排除扫描的文件扩展名以及排除规则应用的扫描类型。

默认情况下，选定的文件扩展名被排除于实时防护和手动扫描，要修改何时应用排除规则，请点击右侧栏并选择所需选项。

点击 下一步。

步骤 4/4 – 选择扫描类型



扫描类型

强烈建议扫描带有指定文件扩展名的文件，以确保它们是干净无毒的。

点击完成。

点击 应用 保存修改。

16.4. 隔离区

BitDefender允许将被感染文件或可疑文件到一个名叫“隔离区”的安全区域。文件被放到隔离区后，将不能感染其他文件，同时您可将它们发送给BitDefender实验室做进一步分析。

要查看和管理隔离的文件或配置隔离区，请到高级视图中的反病毒>隔离区。

BitDefender 全方位安全杀毒软件 - 试用版
切换至基本视图
状态：1 个等待处理的问题
修复
实时防护 病毒扫描 白名单 隔离区
常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册
隔离区

文件名称	病毒名称	位置	发送

设置 发送(S) 恢复(E)
如需获知关于 BitDefender 用户界面各选项的详情，请移动您的鼠标并悬停于相应窗口。此区域将显示相关的帮助文本。
bitdefender
购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

隔离区

隔离区显示所有当前被隔离的文件。 您可看到每个被隔离文件的文件名、感染的病毒、原始路径及提交日期。



注意

当一个病毒被隔离后，就不再有任何危害，因为它将不能被执行和打开。

16.4.1. 管理被隔离的文件

要从隔离区删除选定文件，请点击 删除 按钮。如果您将文件恢复到其原始路径，请点击 恢复。

点击 发送 可以将隔离区内任何选定的文件发送到BitDefender实验室。

右键菜单。. 您可使用右键菜单方便地隔离区文件，上述的选项都可用。您还可点击 刷新 刷新隔离区。

16.4.2. 隔离区设置

要配置隔离区设置，请点击 设置。 接着会显示一个新窗口。



隔离区设置

您可使用隔离区设置选项让BitDefender自动执行以下操作:

删除旧文件。. 要自动删除旧的被隔离文件，请选中相应的选项。 您需要指定要删除的文件存在的天数，以及BitDefender检查旧文件的频率。



注意
默认情况下， BitDefender每天都会将检查旧文件并删除30天以上的文件。

删除重复文件。. 要自动删除重复的被隔离文件，请选中相应的选项。 您必须指定检查重复文件的时间间隔。



注意
默认情况下，BitDefender每天检查重复的隔离文件。

自动提交文件。. 要自动提交被隔离的文件，请选中相应的选项。 您需要指定提交文件的频率。



注意
默认情况下，BitDefender每隔60分钟提交一次隔离区的文件。

升级后扫描隔离区文件。. 要在每次升级后自动扫描隔离文件，请选中检查相应的选项。 如果您想在扫描后自动将安全的文件恢复到原始位置，请选择 恢复安全的文件。

点击 确定 保存修改并关闭窗口。

17. 反垃圾邮件

bitdefender反垃圾邮件雇用了显着的技术创新和行业标准的反垃圾邮件过滤器，以彻底清除垃圾邮件才达到用户的收件箱。

17.1. 反垃圾邮件见解

对个人与团体来说垃圾邮件问题日趋严重。有些色情垃圾邮件,你不希望孩子看到它,你可以应此而恼火(浪费太多时间或在你的办公室邮箱接受到色情邮件),你却不能阻止这些垃圾邮件的发送。 退而求其次,显然就是停止接受。不幸的是,垃圾邮件没有一定的形状和大小而且数目繁多。

17.1.1. 防垃圾邮件过滤器

BitDefender反垃圾邮件引擎包含多种不同过滤器以保护您的收件箱不受垃圾邮件侵扰：好友列表，垃圾邮件发送者列表，字符集过滤器，图像过滤器，URL过滤器，NeuNet(启发式)过滤器 及 贝叶斯过滤器。



注意
在 反垃圾邮件 模块 设置 ，您可以启用/不启用各个过滤器。

白名单/黑名单

通常人们都会与一群一定的人有来往或与某些公司或集团有时常联络。利用 朋友或垃圾邮件发信者单，您可以指定某些您不管内容一律接受邮件的邮址，和指定您向拒绝来信的邮址。

好友列表 / 垃圾邮件发送者列表可以在 高级视图 或集成在邮件客户端软件中的反垃圾邮件工具条 中进行管理。



注意
我们建议您将朋友的名字和电子邮件邮址加入 朋友名单. BitDefender不会拒绝这单内的邮址来信。所以，把朋友加入朋友名单能确保收到合法的邮件。

字符集过滤器

多数的垃圾邮件都是用斯拉夫文和/或亚洲语文编成的。若您想拒绝用这些语文编成的邮件，请利用此过滤器。

图像过滤器

既然如今逃脱启发性过滤器对电脑病毒是很难得，现有的垃圾邮件都多半只拥有非法内容的图影。为了解决这现象，BitDefender采用了 图影过滤器 。此过滤器将邮件内的图影签名和BitDefender档案内的对比。如有类似的，BitDefender将在邮件上打上垃圾邮件的标签。

URL过滤器

多数的垃圾邮件都有连往其他网址的连线（多数都是广告和购物网）。BitDefender有这类型网址的档案。BitDefender会把电子来信内的连线与档案内的对比，如有类似，来信的垃圾分数将。

bitdefender保持一个数据库的这种联系。 URL过滤器检查每一个URL连结在贺电中对自己的数据库。如果匹配的话，这个信息就是，标帜为垃圾邮件。

neunet （启发式）滤波器

启发性过滤器 会在邮件的各个部分进行测试，（除了标题以外，还有ＨＴＭＬ形式或本文形式的主文），寻找有垃圾邮件性态的文字，词句，等。 根据分析的结果，它增加了一个垃圾邮件评分，以讯息。

过滤器还可以检测邮件标记为SEXUALLY-EXPLICIT：明确： 在主题栏和标签，他们为垃圾邮件。



注意

从２００４年，５月１９号起，含有色情内容的垃圾邮件都必须在标题内加入SEXUALLY-EXPLICIT：的词句否则将面对联邦法律的制裁。

贝叶斯过滤器

贝叶斯过滤器 会按照指定文字出现的次数的统计资料和分类邮件。若指定的文字在邮件内的次数符合垃圾邮件内的，邮件将列入垃圾邮件的类型，否则将列入非垃圾邮件类型（按照您或贝叶斯过滤器的指示）。

比如说，要是有四个字在垃圾邮件里经常出现，那接下来内容含有这字的邮件是垃圾邮件的可能性将提高。所有邮件内的相关字都会经过过滤器的计算。垃圾邮件的可能性将以统计资料决定。

此模块还有另一项特别功能：它是能够接受训练的。它能快速的配合用户所收到的邮件类型，存入所有的相关资料。若要有效的运行此过滤器，您必须给予它垃圾邮

件和合法邮件的例子，训练它。在适当的时候，您可能必须更改过滤器的设置，以免它错误认定垃圾邮件。



重要

可以通过 是垃圾邮件 and 不是垃圾邮件 按钮（位于 反垃圾邮件工具条 上）来校正贝叶斯过滤器。



注意

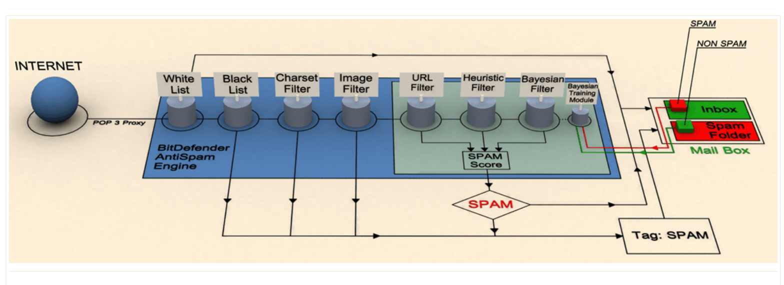
每当您进行更新:

■新的图影签名会加入 图像过滤器.
■新的链接会加入 URL过滤器.
■新的规矩将列入 启发式过滤器.

这些都会帮助提高反垃圾邮件引擎的效率。
为了保护您的系统，BitDefender可以自动更新。请您保持您的 自动更新选项.

17.1.2. 反垃圾邮件设置

以下的图示说明BitDefender如何操作。



反垃圾邮件设置

上图中显示的反垃圾邮件过滤器(好友列表，垃圾邮件发送者列表，字符集过滤器，图像过滤器，URL过滤器，NeuNet(启发式)过滤器 and 贝叶斯过滤器)会被BitDefender反垃圾邮件引擎组合使用，用来判断邮件是否应该被发送到您的 收件箱。

每封来自互联网的电子邮件首先会被 好友列表/垃圾邮件发送者 过滤器检查。 如果发送者的地址存在于 好友列表，邮件会被直接移动到您的 收件箱。

否则 垃圾邮件发送者列表 过滤器会继续检查发送者的地址是否在其列表中。 如果发送者地址在垃圾邮件发送者列表中，则邮件会被标记为“垃圾邮件”并被移动到垃圾邮件 文件夹（位于 Microsoft Outlook）。

否则，charset过滤器将查证电子邮件是否是由西里尔文或亚洲字书写的。如果是，电子邮件将会被移到垃圾邮件箱。

如果电子邮件不是由西里尔文或亚洲字书写的， 就会交给图像过滤. 图像过滤器会检查所有的电子邮件与接收图象信息附载的内容.

URL过滤器会寻找联接,并将发现的联接和BitDefender数据库比较。 如果符合，BitDefende将增加一项垃圾电子邮件。

NeuNet (Heuristic) filter会接收电子邮件,并进行一系列测试,寻找字句或其他垃圾邮件特点。结果是,它会增加垃圾电子邮件标签。



注意

如果电子邮件在标题处被标记为色情的问题,BitDefender会认为是垃圾邮件。

Bayesian的过滤 单元,将进一步分析信息,根据统计资料的速度出现在特定文字信息垃圾分类为垃圾或非垃圾。它会增加垃圾电子邮件分数。

如果总得分(URL评分分数+智慧+Bayesian得分)超过了垃圾信息状态(用户设定的防垃圾邮件为可允许承受能力),被认为是垃圾信息.



重要

如果你不是用微软或微软展电子邮件客户， 你应该有建立一个规则将电子邮件接收的讯息标示加到BitDefender检疫文件。[SPAM] BitDefender附在头的问题[电子邮件]的信息视为垃圾.

17.2. 状态

配置反垃圾邮件保护，点击 反垃圾邮件状态，在设置控制台。

BitDefender 全方位安全杀毒软件 - 试用版　切换至基本视图

状态：5 个等待处理的问题　修复

状态　设置

常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册

反垃圾邮件已启用
好友列表　0 个项目　管理好友
垃圾邮件发送者列表　0 个项目　管理垃圾邮件发送者

防护级别
严格
适度
宽松

介于适度与严格之间
这是推荐的设置。如果您接收到异常多相似的垃圾邮件，请使用此设置。这个设置可能会误报部分正常邮件。配置好友/垃圾邮件发送者列表并训练贝叶斯过滤器将会降低误报的几率。

默认级别

反垃圾邮件统计数据
接收电子邮件 (当前会话)：　0
垃圾电子邮件 (当前会话)：　0
总计接收电子邮件：　0
总计垃圾电子邮件：　0

如需获知关于 BitDefender 用户界面各选项的详情，请移动您的鼠标并悬停于相应窗口。此区域将显示相关的帮助文本。

bitdefender　购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

反垃圾邮件状态

您可以查看是否是隐私控制启用或停用。 如果您想更改反垃圾邮件地位，明确或选择相应的复选框。



重要
防止Spam进入您的 收件箱 ， 保持 反垃圾邮件过滤 使用。

在 统计部分您能观看antispam 活动的结果出席每会议(从您发动了您的电脑) 或总结(从BitDefender 的设施) 。

17.2.1. 配置保护级别

您可以选择最符合您的防护需求的安全级别，上下拖动滚动条以设定最合适的防护级别。

共有5个安全级别:

防护级别	说明
宽松	为收到大量合法商业邮件的帐户提供保护. 过滤器将允许大部分邮件通行,但可能产生被动错误信息(合法信息被错误地标示为垃圾邮件).
允许	为收到合法商业邮件的帐户提供保护. 过滤器将允许大部分邮件通行,但可能产生被动错误信息(合法信息被错误地标示为垃圾邮件).
中等	为常规帐户提供保护. 为了避免把合法邮件过滤, 过滤器只会阻止大多数垃圾邮件。
中度至侵略性	为定期收到大量垃圾邮件的帐户提供保护. 过滤器会让少量垃圾邮件通行,但可能产生错误(合法信息被错误地标示为垃圾邮件). 对好友/垃圾邮件名单 进行设置,并培训学习引擎 (贝叶斯过滤器) 以减少错误数量.
严格	为定期收到大量垃圾邮件的帐户提供保护. 过滤器会让少量垃圾邮件通行,但可能产生错误(合法信息被错误地标示为垃圾邮件). 添加联系人到好友名单的来往以减少错误数量.

设置缺省保护级别 (中度至侵略性) 按 默认级别。

17.2.2. 设置白名单

好友名单 是您总想要收到消息所有电子邮件的名单, 不管他们的内容。消息从您的朋友不被标记作为spam, 既使内容类似Spam。



注意

任一邮件来自地址包含在 好友名单, 自动地将被交付对您的Inbox 没有进一步处理。

要设置好友列表, 请点击 管理好友列表 (或点击 Friends 按钮, 该按钮位于反垃圾邮件工具条上)。





朋友名单

您能补充说或从 好友名单 去除词条。

如果您想要增加 电子邮件.检查 选择, ⊠. 键入地址和点击地址将出现在 好友名单.



重要

句法: name@domain.com.

如果您想要加域名检 域名 选择, ⊠. 键入域名和点击 域名将出现在 好友名单



重要

句法:

- @domain.com, *domain.com 和domain.com – –所有收到的电子邮件从 domain.com 将到达您的 收件箱 不管他们的内容如何;
- *domain* – –所有收到的电子邮件从 域 (无论是否域名结尾) 将到达您的 收件箱 不管他们的内容如何;
- *com – 所有收到的有域名结尾的电子邮件 com 将到达您的 收件箱 不管他们的内容如何;

删除一个项目，从清单中，选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单，但公告：这是不可能收回。

使用 保存/ 载入按钮 保存文件好友列表 . 文件包含.bwl 例外.

选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.



注意

我们建议您将朋友的名字和电子邮件邮址加入 朋友名单. BitDefender不会拒绝这单内的邮址来信。所以，把朋友加入朋友名单能确保收到合法的邮件。

点击 应用 和 好的保存和关闭 好友列表

17.2.3. 配置黑名单

垃圾邮件清单 是您不想要收到消息所有电子邮件的名单，不管他们的内容。



注意

任何一个电子邮件收到从地址包含在 垃圾邮件清单 自动地将被标记作为SPAM ，没有进一步处理。

设置黑名单,点击 管理黑名单 或点击 黑名单按钮,从反垃圾邮件工具条).



垃圾邮件清单

您能补充说或从 垃圾邮件清单 去除词条。

如果您想要增加电子邮件 电子邮件地址 选择, . 键入地址和点击 地址将出现在垃圾邮件列表。



重要

句法: name@domain.com.

如果您想要加域名 选择, .键入域名和点击 域名将出现在 垃圾邮件列表。



重要

句法:

- @domain.com, *domain.com and domain.com – 所有收到的电子邮件从 domain.com 将被标记作为SPAM
- *domain* – –所有收到的电子邮件从 域 (不论是否域名结尾) 将被标记作为SPAM。
- *com – 所有收到的有域名结尾的电子邮件 com 将被标记作为SPAM。

删除一个项目, 从清单中, 选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单, 但公告: 这是不可能收回。

使用 保存/ 载入 按钮保存/ 载入垃圾邮件列表 文件可以.bwl 引伸。

选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.

点击 应用 和 好的 保存和关闭 垃圾邮件清单。



重要

如果您想要重新再安装BitDefender 这是一个好想法保存 好友 / 垃圾邮件 名单前面, 并且在重新安装过程是结束之后您可以装载他们。

17.3. 设置

要配置反垃圾邮件设置及过滤器, 请前往高级视图中的 反垃圾邮件>设置。



反垃圾邮件设置

选择三个类别是可使用的 反垃圾邮件设置 和 基本反垃圾邮件过滤 和 高级反垃圾邮件过滤被组织象一份可伸缩的菜单，相似与那些从视窗。



注意

点击"+" 展开类别或点击"-"收起它。

激活或撤销过滤器选择或清除复选框对应于它。

要应用默认设置，请选中 默认.。

点击 应用 保存修改。

17.3.1. 反垃圾邮件设置

■标记垃圾邮件标题 - 所有电子邮件认为是Spam组用SPAM 将被标记在附属的线。

■在主题上标记phishing – 所有的被认为是phishing电子邮件会被标记为SPAM 在主题行。

17.3.2. 基本反垃圾邮件过滤

■好友/垃圾邮件发送者列表 – 使用 好友/垃圾邮件发送者列表 过滤电子邮件。
- 自动添加受助人的好友名单 –自动添加接受者发送电子邮件给朋友的名单。
- 自动添加到好友列表 – 当您点击 不是垃圾邮件 按钮（位于 反垃圾邮件工具条），该邮件的发件人会被自动添加到“好友列表”。
- 自动添加到垃圾邮件发送者列表 – 当您点击 是垃圾邮件 按钮时（位于 反垃圾邮件工具条）， 该邮件的发件人会被自动添加到“垃圾邮件发送者”列表。



注意
不是垃圾邮件 和 是垃圾邮件 按钮用来训练 贝叶斯过滤器。

■阻止邮件写在亚洲字符 –座讯息写在 亚洲字符集.

■阻止邮件写在西里尔字符 –座讯息写在 西里尔字符集.

17.3.3. 高级防垃圾邮件过滤器

■使学习引擎（贝叶斯） –激活/关闭该 学习引擎（贝叶斯).
- 限制字典大小，以200000字 – 设置Bayesian dictionary – 更小是更加快速的，更大是更加准确的。



注意
推荐大小：200.000 词。

- 培训学习引擎（贝叶斯）对进出的电子邮件 –火车学习引擎（贝叶斯）对进出的电子邮件。

■URL 过滤 – 激活或撤销 URL 过滤.

■neunet （启发式）滤波器 –激活/关闭该 Neunet（启发式）滤波器.
- 阻止明确内容 –激活/失活的检测信息，并露骨性，在主题行。

■图像过滤器 – 激活或禁用图像过滤器.

18. 家长控制

BitDefender家长控制，您可以控制使用互联网，并具体应用为每个用户持有一个用户帐户的系统。

你可以配置家长控制来阻止:

- ■不适当的网页。
- ■互联网接入，为特定的时间内（诸如时间节点） 。
- ■网页和电子邮件，如果他们含有某些关键字。
- ■应用，如游戏，聊天， filesharing程式或其他人。
- ■即时消息发送的即时消息联系人以外的其他允许的。



重要

只有用户具有管理权限时（系统管理员）才可以使用和配置家长控制。 为了确保只有你可以改变设置控制设置,请设置一个密码 当你作为一个特定用户使用家长控制时，你将被提示设定密码。

为了成功地使用家长控制来限制你的孩子的电脑和线上活动，您必须完成这些步骤:

1. 建立有限（标准） Windows用户帐户给您的孩子使用。



注意

要了解如何创建Windows用户帐户，请转至Windows帮助和支持中心（在开始菜单上，单击帮助和支持).

2. 配置家长控制的Windows用户帐户给您的孩子使用

要配置父母控制，进入家长控制在高级显示中。



家长控制

你可以看到家长控制功能为每个Windows用户帐户的现有配置. 双击用户名，打开窗口，您可以为每个用户帐户配置父母控制

这一章中的几个条目中详细介绍了家长控制功能，以及如何配置它们

18.1. 设置每个用户的地位

要配置家长控制特定的用户，双击一个用户，然后双击地位 标签.





家长控制状态

给这个用户帐户配置家长控制，有下面这些步骤:

1. 启用这个用户帐户的家长控制,选择旁边的复选框家长控制.



重要
开启 家长控制,以保护您的孩子浏览不适当的内容，使您的个性化电脑进入正规。

2. 建立一个密码,以保护家长控制设置 欲了解更多信息，请参阅 “保护家长控制设置”（第 180 页).
3. 选择相应的复选框的制度漏洞要定期检查。
   - 网络控制 –过滤网站导航将根据你设置的规则规定网站选项。
   - 应用程序控制－阻止进入你指定的应用程序中应用程序选项
   - 即时通讯控制 – 通过您在 即时通讯通信 部分设置的规则允许或阻止您和特定联系人的聊天。
   - 网页时间限制 －允许网页存取,按照你规定的时间表 时间限制 选项.



■网络接入–阻止进入所有的网站（不只是那些在网站栏目）　。

■关键词过滤 －根据你规定规则过滤网页，电子邮件和即时通讯的获得关键词选项.

■启发式网页过滤 –，过滤网页按照事情确定的规则,根据时间分类。

4. 为了充分受益的特点，所提供的各项父母的控制，你必须配置选定管制。 要了解如何配置它们，请参阅这一章的下列主题.

18.1.1. 保护家长控制设置

如果你是不是唯一的人与行政权的使用这台电脑，我们建议你，保护你的父母控制设置同一个密码。 通过设置一个密码，你将阻止其他用户对行政权力运作，从改变父母控制设置你的配置，为特定的用户。

bitdefender会问你默认设定一个密码时，使家长控制。

BitDefender

如需确保仅有您可以更改家长控制设置，建议您启用密码保护。默认情况下此特性仅将保护家长控制模块，但您可在高级视图窗口中更改此特性。

您想要立即设置密码吗？

密码

重新输入密码

密码必须至少包含 8 个字符。

☐ 启用家长控制时不询问密码

确定(O)　取消(C)

启动密码保护

设置密码保护有以下内容:

1. 键入密码，在 密码区。
2. 再次输入密码，在 再次输入密码 实地证实。



3. 点击 好的 来保存密码和关上视窗。

一旦你设定密码，如果您想改变父母控制设置，你将会被要求提供密码。 其他的系统管理员（如果有的话）也将提供这方面的密码，以改变家长控制设置。


注意
此密码将不会保护其他bitdefender设置。

如果您不要设定一个密码，你不希望这个窗口再出现，检查 不要问一个密码时，使家长控制

18.1.2. 配置启发式Web过滤

启发式网页过滤分析网页并阻挡那些匹配模式的潜在不适当的内容。

为了过滤网络接入按照预先确定基于年龄的规则集，你必须确定一个具体容忍的水平。 拖曳滚动条为指定用户设定防护级别.

共有3个安全级别:

安全级别	说明
儿童	根据对14周岁以下用户的推荐设置,限制网页访问. 阻止含有对儿童可能有害内容的网页(色情、性、毒品、打杀等）.
少年	根据对14-18周岁用户的推荐设置,限制网页访问. 阻止所有关于性、色情作品或成人内容的网页.
成人	无论网页内容是什么,不限制访问所有网页.

点击 默认级别 定滑块在默认级别。

18.2. 网路控制

网络监控 帮助您阻止访问有不适当内容的站点。BitDefender会提供一份要阻止的网站站点和网页的名单，同时BitDefender也会不时更新此名单。您可以选择是否阻止那些含有在黑名单上站点链接的网页。

要配置网络控制特定的用户，双击目标用户，并点击 网络标签.

网路控制

要启动这个保护，请选中相应 启动网络监控的检验盒。

通过选择跟 指定被允许的网站 指定被阻止的网站 相应检验盒来允许/ 阻止访问在步骤二指明的网站。

规则必须手动输入。首先，选择 允许访问这些网页的 / 阻止访问这些网页 ，以许可证/块进入该网站你会在向导。然后，点击 放入 按钮启动配置向导。

要削除规则，选择它并且点击 删除按钮。要削除所有规则，进入 显示并且点击 清楚 的按钮。修改规则精选它和点击 编辑 按钮。暂时地解除一个规则并没有削除它，清除对应的复选框。

点击 应用 保存修改。

18.2.1. 配置向导

配置向导是一个1步骤程序。

步骤1— 特殊网站

BitDefender - 网站向导

输入 URL

您可以输入单独的网页地址或者有通配符的地址。

例如，通过在指定区域内输入*cigars*，您可以阻止所有含有'cigars'这个词的地址。

完成 取消

特殊网站

键入网址，其中的规则，将适用并点击 完成.



重要

句法:

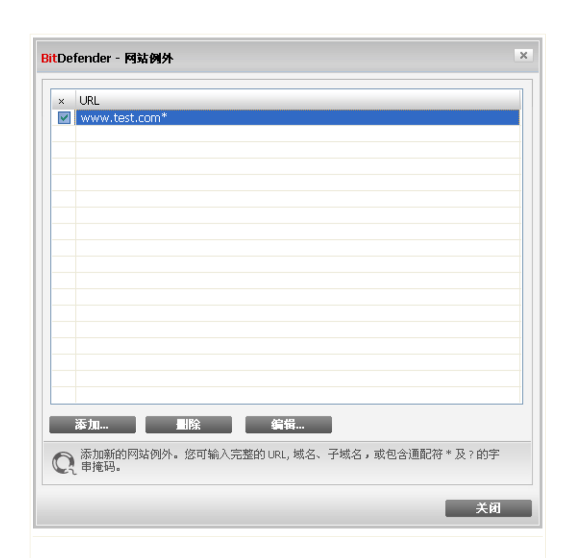
- *.xxx.com – 此规矩的措施将会应用在所有以 .xxx.com:作为结尾的网站;
- *porn* – 此规矩的措施将会应用在所有含有 porn在其网址的网站;
- www.*.com – 此规矩的措施将会应用在所有以 com;
- www.xxx.* – 此规矩的措施将会应用在所有以www.xxx. 作为开头无论任何领域结尾的网站;

18.2.2. 具体例外

有时您可能需要对某一规则明确它的例外.例如,您设置阻止所有含有关键词"Killer"(syntax: *killer*)的网址.您必须注意有一个叫killer-music的在线音乐网页是不用阻止的.进入排除界面能指定以前建立的规则的排除项.

点击例外。 以下的视窗会打开:





具体例外

点击 添加... 将出现一个 设置向导 界面,可以指定要排除的网址.完成该向导就能设定要排除的网址.

要删除一个规矩，只要选中它并单击 删除。要修改一个规矩，选中它并单击 编辑或双击它就可。要在不删除一个规矩时暂时不启动它，只要不要选中它相应的检验盒就可。

点击 关闭 保存更改并关闭窗口。

18.2.3. BitDefender 网页黑名单

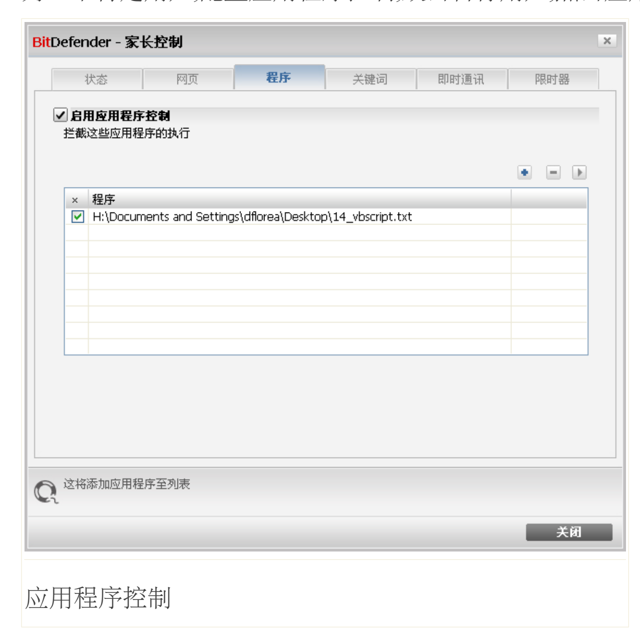
为了帮助您保护孩子,BitDefeder提供了一个含有不当或潜在风险内容网页的黑名单.选定使用BitDefender提供的网页阻止名单可以阻止这个名单中出现的网址.

18.3. 应用程序控制

应用程序监控 帮助您阻止任何的应用程序运行。这样，游戏，多媒体和信息软件，还有其他种类的软件和恶意软件都会被阻止。用这样的方式阻止应用程序也同样的保护了应用程序不会被修改，不可以被复制或移动。



为一个特定用户,配置应用程序控制,双击目标用户,点击应用程序标签.



应用程序控制

选中与 启动应用程序监控 相应的复选框（checkbox）以启动此保护。

规则必须手动输入。点击 增加... 按钮来启动配置向导。

要删除规则，选择它并且点击 删除按钮。要删除所有规则，进入 显示并且点击 清楚 的按钮。修改规则精选它和点击 编辑 按钮。暂时地解除一个规则并没有削除它，清除对应的复选框。

点击 应用 保存修改。

18.3.1. 配置向导

配置向导是一个1步骤程序。

步骤一 — 选择要被阻止的应用程序

选择要被阻止的应用程序

单击 浏览，然后选择要被阻止的应用程序，最后单击 完成。

18.4. 关键词过滤

关键字过滤可以帮助您阻止用户对电子邮件，网页和即时信息中一些特定的字词。使用关键字过滤，您的孩子当他们在线时可以防止看到不恰当的字词或短语.



注意

即时消息关键字过滤仅适用于雅虎Messenger和Windows Live （微软）

如果要给特定的用户设定关键字过滤，双击目标用户，然后点击关键字 标签.

关键词过滤

选择 启用关键字过滤 查看复选框,如果你想用这个控制功能.

您必须添加规则，指定的关键字将被封锁 要添加规则，请点击 添加 按钮并在设置窗口中配置规则的参数。

要删除一个规则，选中它并点击 删除 按钮。 要编辑已有的规则，请双击改规则或者点击 编辑 按钮并在设置窗口进行所需的修改。

点击 应用 保存修改。

18.4.1. 设置窗口

当您添加或修改的规则时,配置窗口就会出现。

BitDefender - 关键词向导
添加新的关键词
test
选择选项
HTTP
POP3
即时通讯
全词匹配
请添加需要拦截而不显示的关键词（整个邮件及网页都将被拦截）。
添加关键词至此列表，所有包含这些关键词内容的站点和电子邮件将被拦截访问
完成 取消

输入关键字

您必须设置以下参数:

■关键字 -类型，在编辑领域中输入你想禁止的字或词语。
■协议 -选择议定书BitDefender要扫描特定单词。

选项	说明
POP3	含有这个关键词的邮件将被阻止.
HTTP	含有这个关键词的网页将被阻止.
进入	即时消息中包含设定的关键字将被阻止

点击 完成来添加规则。

18.5. 即时消息（ IM ）控制

即时消息（ IM ）控制让您可以指定您的孩子只和被允许的对象聊天。





注意

即时通讯控制仅适用于雅虎Messenger和Windows Live （微软）Messenger.

如果要设定即时控制特定的用户帐户，双击目标用户，并点击IM流量标签.

BitDefender - 家长控制

状态 | 网页 | 程序 | 关键词 | 即时通讯 | 限时器

启用即时通讯控制

拒绝或允许与下列即时通讯联系人聊天：

联系人名称	即时通讯程序	操作
testauto@live.com	MSN	允许

拦截列表以外的所有即时通讯用户

此列表将显示所有被允许或拦截的即时通讯联系人。

关闭

即时聊天控制

选择 启动即时消息控制 复选框。

您必须添加规则用以指定哪些即时聊天用户允许或不允许聊天. 要添加规则，请点击 添加 按钮并在设置窗口中配置规则的参数。

要删除一个规则，选中它并点击 删除 按钮。 要编辑已有的规则，请双击改规则或者点击 编辑 按钮并在设置窗口进行所需的修改。

如果您已经确定所有IM接触用户可以聊天，选择让所有的IM用户通过. 通过这种方式，可以明确即时聊天允许传送信息的用户

点击 应用 保存修改。

18.5.1. 设置窗口

当您添加或修改的规则时,配置窗口就会出现。

添加聊天联系人

以下步骤:

1. 输入即时通讯联系的用户名称（ID）
2. 选择即时通讯项目的联系人
3. 选择规则
   - ■拒绝这个聊天联系
   - ■允许这个聊天联系
4. 点击　完成来添加规则。

18.6. 上网限时器

指定地时间段里，网络限时器 帮助你允许或禁止用户或应用程序访问网络.



注意

BitDefender 将会不时更新，无论什么样的 网络限时器 设置。

要为特定的用户配置网络时间限，双击目标用户，并点击 时间限制标签.



上网限时器

为了启动这种保护,选中相应的复选框启动网络限时器。

当所有的网络连接将全被阻止时，检查所有请选择一个时间间隔。不检查所有您可以单击单元格或以单击及拖动的方式来更长的时间。



重要

灰色的方框代表着所有网络连接被禁止的时间。

点击 应用 保存修改。

19. 隐私控制

BitDefender监控着您系统中可能被间谍软件利用的“热点”，同时检查所有对您的系统和软件的修改。这可有效阻止黑客安装在系统中的木马和其他恶意软件，保护您的私密信息不被窃取（如信用卡号码等）。

19.1. 隐私控制状态

要配置隐私控制或查看其信息，请到高级视图中的 隐私控制>状态。



隐私控制状态

您可以查看隐私是启用还是禁用。 如果您想更改隐私控制状态，请清除或选中对应的复选框。



重要
为防止您的私密资料失窃，保护您的隐私，请保持启用 隐私控制。

隐私控制采用下列的防护控制保护您的计算机：

- 个人信息控制 – 过滤所有发出的网页（HTTP）和电子邮件（SMTP）及即时通讯流量以保护您的私密数据，您可在 个人信息 部分设置过滤规则。
- 注册表控制 – 当应用程序试图修改注册表项以在系统启动时自动执行时，征询您的许可。
- Cookie控制 – 当新网站试图设置Cookie时，征询您的许可。
- 脚本控制 – 当网站试图运行一个脚本或其他活动内容时征询您的许可。

在窗口的底部您可看到 隐私控制统计。

19.1.1. 设置防护级别

您可以选择最符合您的防护需求的安全级别，上下拖动滚动条以设定最合适的防护级别。

共有3个防护级别：

防护级别	说明
宽松	仅注册表控制 启用。
默认	注册表控制 和 个人信息控制 启用。
严格	注册表控制 个人信息控制 和 脚本控制 启用。

您也可点击 自定义级别 自己定义防护级别。 再接下来出现的窗口中选择您想启用的防护控制并点击 确定。

点击 默认级别 将滚动条放到默认级别位置。

19.2. 个人信息控制

保证私密数据的安全是一个困扰我们的大问题。数据失窃随着互联网通讯的发展而愈加严重，并利用最新技术欺骗用户交出私密信息。

无论是您的电子邮件或信用卡号码，只要它们落入了恶意之手，就会给您带来损失：您可能会发现自己淹没在垃圾邮件中，或者发现巨额的信用卡消费。

隐私控制保护您的敏感数据免受在线窃取。 基于您创建的规则，隐私控制扫描从您计算机发出的网页、电子邮件和即时通讯通信中是否包含特定字符串（例如，您的信用卡号码）。如果发现匹配，则对应的网页、电子邮件或即时讯息会被阻止。

您可创建规则来保护您认为需要保密的任何信息，比如电话号码、身份证号码、银行卡号、电子邮件地址等。 本功能支持多用户，使用不同的Windows用户账户登录可以设置不同的个人信息防护规则。 只有当您登录到自己的Windows用户账户后，您所创建的规则才会被应用和访问。

为什么使用个人信息控制?

■ 个人信息控制可以非常有效地阻止记录键盘敲击的间谍软件。 这种类型的恶意软件记录您的击键顺序并通过互联网将记录发送给黑客。 黑客可以从获得的记录中找出敏感信息，例如银行卡号和密码，并从中获利。

  假设这样的应用程序设法避免了被杀毒软件检测到，但是您创建了合适的个人信息保护规则，那么该程序还是无法通过电子邮件、网页或即时通讯将偷窃的数据发送出去。

■ 个人信息控制还可以保护您免受 钓鱼 侵害（试图窃取个人信息）。 最常见的钓鱼式攻击企图利用欺骗性的电子邮件，引诱你在一个虚假的网页上提交个人信息。

  例如，您可能会收到一封电子邮件，声称是来自您的银行，并请您立即更新您的银行帐户信息。 电子邮件中提供了到银行网页的链接，让您去那里提交个人信息。 虽然它们看起来是合法的，但是电子邮件中链接指向的网页是虚假的。 如果您点击电子邮件中的链接并在虚假网页上提交了您的个人信息，您就会把自己的个人信息发送给了设计这个钓鱼欺骗的黑客。

  但是如果您已经设置了合适的个人信息保护规则，除非您设置了例外，否则您就不能通过网页提交您的个人信息数据。

要配置个人信息控制，请到高级视图的 隐私控制>个人信息 标签页。

个人信息控制

如果您想要使用的隐私控制，请执行下列步骤：

1. 选中 个人信息防护 复选框。
2. 创建规则以保护您的敏感数据。 欲了解更多信息，请参见 “创建个人信息控制规则” （第 195 页）。
3. 如果需要，请为您创建的规则定义特定的例外情况。 欲了解更多信息，请参阅 “定义例外” （第 199 页）。

19.2.1. 创建个人信息控制规则

要创建个人信息保护规则，请点击 ▪ 添加 按钮，并按照配置向导的引导进行操作。

步骤 1/4 - 欢迎窗口

BitDefender - 个人信息控制规则向导

个人信息控制模块会监视HTTP（网络）和SMTP（电子邮件）的流量，过滤您计算机中私人信息——比如信用卡号码，和其他用户自定义字符串（如密码）。

向导会引导您完成所需步骤，以创造管理规则。这也可从"高级视图>隐私控制">，点击在上面部分的隐私控制选项卡上的"添加规则"图标。

下一步 取消

欢迎窗口

点击 下一步。

步骤 2/4 – 设置规则类型和规则数据

BitDefender - 个人信息控制规则向导

规则名称

规则类型 Pin 码

规则数据

个人信息已被加密且其不可被除了您以外的任何人使用。如需获得更高的安全性，请仅输入所需保护的信息的部分内容（示例：如需过滤邮箱 john.doe@example.com 的通信，您仅应在目标字串中输入 "john"）。

在此输入规则名称

上一步 下一步 取消

设置规则类型和规则数据

您必须设置以下参数:

- 规则名称 – 请在此输入规则的名称。
- 规则类型 – 选择规则类型（地址、姓名、信用卡、身份证等）。
- 规则数据 – 请输入您希望保护的数据。 例如，如果您要保护您的信用卡号码，请在这里输入信用卡号码的全部或部分数字。



注意

如果您输入的字符少于三个，系统会提示您验证数据。我们推荐您输入至少三个字符，以避免误拦截网页或电子邮件。

所有您输入的数据都会被加密，为了加强安全性，请不要输入您要保护的信息的全部数据。

点击 下一步。

步骤 3/4 – 选择要检查的通信类型

BitDefender - 个人信息控制规则向导

扫描 HTTP
扫描 SMTP
扫描即时通讯

全词匹配
区分大小写

即时通讯程序通信若包含您的个人信息将会被拦截。

勾选可启用 HTTP 通信扫描

上一步 下一步 取消

选择通信类型

选择您希望BitDefender扫描的通信类型。 您可选择以下任务:

■扫描HTTP – 扫描HTTP（网页）通信并阻止匹配上了规则的发出数据。

■扫描SMTP – 扫描SMTP（电子邮件）通信并阻止要发出的匹配上了规则的电子邮件。

■扫描即时通讯 – 扫描即时通讯流量并阻止要发出的包含规则数据的聊天信息。

您可以仅当规则全部匹配字符串或大小写匹配字符串时应用此规则。

点击 下一步。

步骤 4/4 – 规则说明

BitDefender - 个人信息控制规则向导

规则描述

请为此规则输入描述。描述信息可帮助您或其他管理员轻松识别您所拦截的信息。

请为此规则输入描述

上一步 完成 取消

规则说明

在编辑框中输入对此规则的简短说明。 由于当您查看规则时，需要被被阻止的数据（字符串）不是明文显示的，规则说明能帮助您了解该规则的用途。

点击完成。 规则将会显示在表格中。

19.2.2. 定义例外

有时需要为特定的隐私规则定义例外条件。 例如，您定义了一个规则，以防止您的信用卡号码被通过HTTP（网页）发送出去。这样每当您在一个网站提交信用卡号码时，该网页都会被拦截。如果您想在购物网站上购物，您就必须为这个规则指定一个例外。

要打开管理例外的窗口，请点击例外。

扫描白名单

要添加例外，按照下列步骤进行：

1. 点击 添加 在表中添加一个新条目。
2. 双击 指定允许的地址 并输入您想添加为例外的网址、电子邮件地址或即时通讯联系人。
3. 双击选择类型，并从菜单中选择和之前输入的地址对应的类型。
   - 如果您指定的是一个网站地址，请选择HTTP。
   - 如果您指定的是一个电子邮件地址，请选择SMTP。
   - 如果您指定了即时通讯联系人，请选择 即时通讯。

要删除一个例外条目，请从列表中选中它然后点击 删除。

点击 确定 保存修改。

19.2.3. 管理规则

您可在列表中看到已创建的规则。

要删除一个规则，选中它并点击 删除 按钮。



要编辑规则，请选中并点击 ▷ "编辑" 按钮或双击它，一个新的窗口会出现。



编辑规则

您可在此修改规则的名称、说明和参数（规则类型、规则数据和扫描的通信类型）。点击确定 以保存更改。

19.3. 注册表控制

Windows操作系统有个非常重要的组件叫 注册表，Windows在此记录其设置选项、已安装的程序、用户信息及其他很多信息。

注册表　还被用作定义哪些程序在Windows启动时会自动启动，病毒经常利用这一点以便在用户重启电脑时自动加载。

注册表控制　监控Windows注册表，这对检测木马程序也很有用。每当一个程序试图修改注册表以便在Windows启动时被加载时，您都会得到警告。





注册表警告

您可看到试图修改Windows注册表的程序名称。

如果您不清楚该程序，或者该程序看起来可疑，请点击 拦截 防止它修改Windows注册表。 否则，请点击 允许 允许修改。

根据您的选择，会创建一条规则并显示在规则表中。 以后每当此程序试图修改注册表时，会应用同样的操作选项。



注意

通常在您安装需要在下次系统重启时运行的新软件时，BitDefender都会警告您。绝大多数情况下，这些程序是合法的，可以被信任。

要配置注册表控制，请到高级视图中的 隐私控制>注册表。

注册表控制

您可在列表中看到已创建的规则。

要删除一个规则，选中它并点击 ⊟ 删除 按钮。

19.4. Cookie控制

Cookie 在互联网中非常常见。它们是存储在您计算机上的小文件，您访问的网站在您的计算机上创建Cookie文件以记录您的特定信息。

Cookie 的主要目的是让您访问网站更方便，例如，网站可以借助Cookie记住您的姓名和偏好，这样您不必在每次访问该网站时都输入这些信息。

但是Cookie同样可以被用作跟踪您的上网习惯，从而触及您的隐私。

这就是 Cookie控制 的作用。启用 Cookie控制 后，每当一个新网站试图在您的计算机上设置Cookie时，都会征询您的许可：



Cookie警报

您能看到试图设置或发送Cookie文件的程序名。

选中 记住我的选择 选项并点击是 或 否，就会在规则表中创建一条规则并应用它。下次您访问此网站时将不会被提示。

您可用这个功能选择信任和不信任的网站。



注意

由于互联网上巨量的Cookie被使用，Cookies控制 开始使用时可能相当烦人，因为开始时它会询问很多有关某网站要在您的计算机上设置Cookie的问题。不过当您把您常用的网站都添加到规则表中后，上网就会变得和以前一样方便。

要配置Cookie控制，请到高级视图中的 隐私控制>Cookie。



Cookie控制

您可在列表中看到已创建的规则。



重要

规则按照优先级高低从上到下排列，最上面的规则有最高优先级。您可拖放规则改变其优先级。

要删除一个规则，选中它并点击 ⊟ 删除 按钮。 如果要修改规则的参数，双击该规则，然后在设置窗口做必要的修改。

要手动添加一条规则，请点击 ⊞ 添加 按钮，并在设置窗口中配置规则参数。

19.4.1. 设置窗口

当您编辑或手动添加一条规则时，设置窗口就会出现。

BitDefender - Cookie 规则向导

输入域名
- 全部
- 输入域名

选择操作
- 允许
- 拒绝

选择方向
- 发送
- 接收
- 两者

选择需要允许或拒绝 Cookie 的网站及域名。Cookie 用于跟踪上网行为及其它信息。请注意，部分网站若无 Cookie 将无法正常运行。

输入域名 URL

完成 取消

选择网址、操作和方向

您可以设定下述参数:

■域名 – 输入要应用规则的域名。
■操作 – 选择规则的操作。

操作	说明
允许	允许该域名上的Cookie操作。
拒绝	不允许域名上的Cookie操作。

■方向 – 选择通信的方向。

类型	说明
发送	规则只对发向网站的Cookie生效。
接收	规则只对接收自网站的Cookie生效。
两者	规则对发送和接收的Cookie都生效。



注意
您可通过设置操作 否，方向为 发送 以实现只接收Cookie但是从不向网站发送Cookie。

点击完成。

19.5. 脚本控制

脚本 及 ActiveX控件和Java applets 等代码被用于创建交互式网页，它们可被编写为具有危害行为。例如，ActiveX控件可以获取对您计算机数据的完全控制，可以读取您的数据、删除信息、截获密码并截取您上网时的邮件。您应当只接受来自您信赖网站的脚本。

Bitdefender可让您选择运行此类脚本或阻止其执行。

借助 脚本控制，您可控制您信任和不信任哪些网站。每当一个网站试图运行脚本或其他活动内容时，BitDefender会征询您的许可：



脚本警报

您可看到脚本资源的名称。

选中 记住我的选择 选项并点击 是 或 否 会在规则表中创建一条规则并应用它。下次当同一个网站试图执行活动内容时将不会再提示您。

要配置脚本控制，请到高级视图中的 隐私控制>脚本控制。



BitDefender 全方位安全杀毒软件 - 试用版
切换至基本视图
状态：4 个等待处理的问题
修复
状态 个人信息 注册表 Cookie 脚本
常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册
启用脚本控制
被拦截的脚本总数： 0

域名	操作

勾选此框可启用脚本控制。这将提示您允许或拒绝诸如 ActiveX 控件、Java 脚本及小程序、VB 脚本之类的脚本。恶意脚本将危及您的系统安全。建议拦截所有您不信任的域名的脚本。
bitdefender
购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

脚本控制

您可在列表中看到已创建的规则。



重要
规则按照优先级高低从上到下排列，最上面的规则有最高优先级。您可拖放规则改变其优先级。

要删除一个规则，选中它并点击 ⊟ 删除 按钮。 如果要修改规则的参数，双击该规则，然后在设置窗口做必要的修改。

要手动创建规则，请点击 ⊞ 添加 按钮并在设置窗口中配置规则参数。

19.5.1. 设置窗口

当您编辑或手动添加一条规则时，设置窗口就会出现。

BitDefender - 脚本规则向导

输入域名

选择操作

允许

拒绝

选择您允许或阻止脚本运行的特定域名。
通常，您可以使用此向导来指定您允许脚本运行的域名。我们建议您阻挡所有您并不十分信赖的域名的脚本运行。

输入域名 URL

完成 取消

选择域名和操作

您可以设定下述参数:

■域名 – 输入要应用规则的域名。
■操作 – 选择规则的操作。

操作	说明
允许	该域名上的脚本将被执行。
拒绝	该域名上的脚本将不会执行。

点击完成。

20. 防火墙

电脑防火墙保护避免擅自进出的联接尝试。 这是一个类似在你门口守卫--它将密切注视和确保谁可以连接互联网



注意
如果你有宽频或数字用户线路，防火墙是必不可少的。

在秘密模式中,用户的电脑将会被隐藏在恶意软件和黑客之外。防火墙模块能自动发现和防护端口扫描(通常黑客准备攻击电脑前,会对电脑发送许多程序包以发现"进入点").

20.1. 设置

配置防火墙保护，进入 防火墙设置 在高级浏览。



防火墙设置

你可以看到BitDefender防火墙是否启用或禁用. 如果您想更改防火墙的状态,请选择相应的复选框.



重要

请保持防火墙 启以防止网路攻击

两个类别信息:

■网络配置简介. 您可以看到您的计算机的名称，其IP地址和默认网关 如果你有多个网络适配器（也就是说，您已连接到多个网络），您会看到每个网络适配器的IP地址和网关配置

■统计. 你可以看到防火墙活动的各种统计数据。

・发送的字节

- 收到的字节
- BitDefender端口扫描数值检测并阻止。 端口扫描往往是黑客用来寻找计算机上的开放端口,用以利用它们。
- 下载数据包的数据
- 开放端口的数据
- 主动传入连接的数据
- 主动输出连接的数据

要查看活动连接和打开的端口，请前往 活动 标签页。

在底下部分您能看BitDefender 统计关于接踵而来和外出的交通。图表显示互联网话务量在前二分钟期间。



注意
图表出现既使 防火墙 是解除的。

20.1.1. 设置默认的行动

默认情况下， BitDefender自动允许所有从白名单访问网络服务和互联网的已知的程序. 对于所有其他程序， BitDefender将会通过一个警示窗口提示您，指定要采取的行动。 您指定的行动适用于每一次目标应用程序要求网络/互联网接入

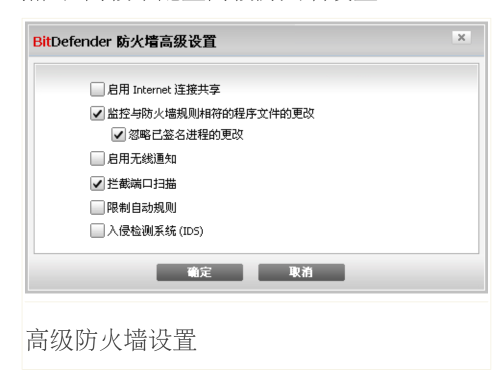
您可以通过拖动滑块来设置对应用程序的连接要求采取的默认行动。 以下默认行动是可用的:

默认行动	说明
允许所有	适用于目前的规则，并允许所有车辆的企图不符合任何现行规则没有提示。 这项政策是极力劝阻，但也可能是有用的，为网络管理员和玩家
允许已知的项目	适用于目前的规则并且允许从合法的（白名单）的程序发送的连接尝试 ， 不需要提示。至于其余的连接尝试，BitDefender将会征求您的同意。 安全名单程序是全世界最常用的应用程序.它们包括最常见的网页浏览器、视听程序、图像播放器、聊天软件和文件共享程序，以及服务器客户和操作系统程序。

默认行动	说明
报告	适用于目前的规则，并征询大家对所有车辆的企图不符合任何现行规则。
拒绝所有	应用于目前的规则，并否认企图不符合任何现行规则的所有流量。

20.1.2. 配置高级防火墙设置

点击 高级来配置高级防火墙设置。



高级防火墙设置

您可选择以下任务:

■启用Internet连接共享（ ICS ）的支持 – 可以支持Internet连接共享（ ICS ）。



注意

允许网络连接共享.该选项不会自动开启用户系统上的网络连接共享功能,只会在用户从操作系统中开启后才允许这类连接.

网络连接共享使本地网络成员能通过您的电脑连接到网络.当您受益于某种特定/特殊的网络连接方式(如无线网络),想让其他成员也共享您的网络时,网络共享是十分实用的.

与本地网络中的成员共享您的网络连接将导致消耗更多的资源并带来一定的风险.这还将打开您电脑的一些端口(被使用您电脑连接的成员打开)

■监察变化程序文件相匹配的防火墙规则 -检查每一个应用试图连接到网际网路，看看是否已经改变，因为规则控制其准入补充。如果该申请已变了，一个警示，将提示您是否允许或阻止访问的应用到互联网。

一般情况下，申请改变更新。但是，有一种风险是，他们可能会有所变化，由恶意软件应用，其目的是感染您的计算机和其它计算机网络。



注意
我们建议你把这个选项选中，并允许进入的只是那些申请你期待已改变后的规则控制他们获得创造。

签署的申请是为了可以信赖的，具有更高程度的安全性。 你可以查阅 忽视的变化，签署过程 ，以使改变签署应用连接到互联网，没有你的手中接到了警报关于此事件。

■启用无线网络通知 - 如果您连接到一个无线网络，程序会显示一个信息窗口，通知您特定的网络事件（例如，有新电脑加入此无线网络等）。

■阻止端口扫描检测和拦截那些试图找出开放端口的程序

端口扫描往往是黑客用来找出在您的电脑上哪些端口是开放。 然后，如果他们找到一种不太安全或很脆弱的端口,他们可能会通过它闯入您的计算机。

■精密的自动规则 - 使用防火墙警报窗口建立精密的规则 在这个选项中,BitDefender将提示您所需要进行的行动,并为每一个不同应用程序网络或互联网接入服务的进程建立规则

■入侵检测系统(IDS) - 启用启发式程序监测，监控试图访问网络服务或互联网的程序。

20.2. 家庭网络

要配置防火墙设置,进入防火墙,网络 在高级浏览中.



家庭网络

该栏目中的网络设置 表提供详细资料，你的网络连接到:

■适配器 – 网络适配器使您的计算机能够连接到网络或互联网

■类型 –信任级别分配给网络适配器。 根据不同的网络适配器配置， BitDefender 会自动给适配器一个信任等级级或提示您提供更多的信息。

■隐身 – 是否您不能被其他计算机检测到。

■通用 是否通用规则适用于此

■地址 – 在适配器上设置IP地址。

■网关 –你电脑的IP地址用于连接网络。

20.2.1. 改变信任等级

BitDefender给予每个网络适配器一个信任等级 适配器上的信任等级表明了每个网络的信任度。

基于信任的水平，具体的规则被适配器创建如何让系统和BitDefender进程访问网络和互联网。

您可以在网络设定 表中看到全部适配器的信任级别，该级别显示在 类型 列。 要更改信任等级，单击箭头从类别栏中选择自定义等级

信任级别	说明
完全信任	目标适配器禁用防火墙
被信任的本地	允许你的计算机和别的计算机所有的本地网络流量
安全	允许本地网络的计算机共享资源。 这个级别会自动设定为当地（家庭或办公室）网络.
不安全	停止网络或Internet计算机连接到您的计算机。 这个级别会自动为公共网络设置（如果你从一个互联网服务提供商收到一个IP地址） 。
本地网络被阻止	阻止所有在您的计算机和局域网络内的其他计算机之间流量，同时提供互联网接入服务。 这个信任等级将会为无担保的(开放的)无线网络自动进行设置
被阻止	通过选定的适配器完全封锁网络和互联网流量。

20.2.2. 配置隐身模式

隐身模式将您的计算机隐藏于网络或互联网,这将免受恶意软件和黑客的攻击 要配置静默模式，请点击 ▾ 静默 列上的箭头并选择所需选项。

隐身选项	说明
打开.	隐身模式已开启。 在本地网络和互联网上,您的计算机将会是不可见的
关闭	隐形模式已关闭。 任何人可以都从本地网络或互联网检测到您的电脑

隐身选项	说明
远程	您的计算机无法从互联网上被检测到 本地网络用户可以检测到您的电脑。

20.2.3. 配置常用设置

如果网络适配器的IP地址改变， BitDefender将会修改相应的信任水平。 如果您想保持相同的信任等级，请点击 ▾通用 列上的箭头并选择 是。

20.2.4. 网络区

你可以为特定的适配器添加允许或阻止.

一个信任的区域的一台电脑，你已经完全信任 你的电脑和被信任的电脑将被允许所有的数据流量 与特定的计算机在一个无担保的无线网络分享资源，请将它们添加为被允许的对象。

一个被阻止的区域的一台电脑，将不能与您域内的任何一台电脑连接

区域 –表中显示当前的网络区域的每个适配器

要添加一个区域，请点击 ▪ 添加 按钮。



添加区域



以下步骤:

1. 选择您想添加的电脑的IP地址
2. 选择措施
   ■允许 – 允许您的计算机与选定的计算机的所有流量
   ■拒绝阻止您的计算机与选定的计算机的所有流量
3. 点击 确定。

20.3. 规则

管理防火墙规则控制,应用程序访问网络资源和互联网, 进入防火墙规则 在高级浏览中。



防火墙规则

你可以看到已经为应用程序（进程）建立的防火墙规则 清除隐藏系统规则 复选框 如果您想看到规则系统或BitDefender的进程

要查看为特定应用程序创建规则，请点击相应程序边上的方框 您可以了解每条规则的详细信息，如表列

■进程/适配器类型 – 应用于进程和网络适配器的规则。 规则自动为任一适配器创建过滤网络或互联网接入。 您可以手动创建规则或修改现有规则，以通过一个特定的适配器过滤应用程序的网络或互联网接入（例如，一个无线网络适配器） 。

■指令栏–从Windows命令行界面启动,该命令用于启动进程（cmd).

■协议 – 规则应用的IP协议。 你可以看见以下的任何一步:

协议	说明
任何	包括所有IP协议
TCP	TCP（传输控制协议）使二个主机建立连接并且交换数据. TCP保证数据转送，同时保证那数据包将按照原样被转送。
UDP	UDP（用户数据协议）是基于IP 运输设计为高性能项目的。游戏和其他录影基础也使用UDP.
一个数字	代表一个特定IP协议（除TCP和UDP ） 。 你可以找到已分配的IP协议号码的完整名单www.iana.org/assignments/protocol-numbers.

■网络事件 – 网络活动的规则应用于。 下列事件可能考虑到:

事件	说明
连接	初步交换了标准信息所使用的面向连接的协议（如TCP ） ，以建立一个连接。 随着面向连接的协议，在连接建立之后的两台有数据通信的计算机之间。
通信	数据流通的两台计算机之间
注意	在这个状态里,有一个应用程序监控这个网络并等待来建立一个和同等的应用程序的连接,或从这个同等的应用程序接收信息

■当地端口 – 您计算机上应用规则的端口

■远程端口 –远程计算机上应用规则的端口



■当地 –是否规则仅适用于本地网络的电脑中。

■行动 –在特定情况下申请是否被允许或拒绝访问网络或互联网.

20.3.1. 自动添加条例

与 防火墙 使用，每当与互联网的联系被建立，BitDefender将请求您的允许:



防火墙警告

您能看以下: 设法访问互联网、协议 地址和应用软件设法连接的 端口。

点击 允许 ，让所有交通（呼入和呼出）上产生的这种应用，从本地主机向任何目的地，在各自的IP协议，并在所有港口。如果你点击 阻止，申请将被拒绝进入互联网超过各自的IP协议完全。

根据你的回答，一项规则，将可创造，应用和列于附表。未来时间的应用会试图连接，这条规则将适用于默认。



重要

允许入站连接企图只从您明确地信任的IP’s或您明确地信任的域名。

20.3.2. 删除规则

要删除一条规则，请选中它并点击 ⊟ 删除规则 按钮。 您一次可以选择并删除一些规则.

如果您想删除为某个应用程序创建的所有规则，请从列表中选择该应用程序，然后点击 ⊟ 删除规则 按钮。

20.3.3. Creating and Modifying Rules

在配置规则中的参数配置窗口中,手动创建新的规则并修改现有规则。

创建规则. 要手动创建一个规则，请按照下列步骤:



1. 点击 添加规则 按钮。 配置窗口将会显示。
2. 如需要，可以配置主要内容和高级参数
3. 点击 好的 添加新的规则

修改规则. 如果要修改现有规则，执行下列步骤:

1. 点击 编辑规则 按钮或双击该规则。 配置窗口将会显示。
2. 如需要，可以配置主要内容和高级参数
3. 点击 确定 保存修改。

配置主要参数

主要 配置窗口的标签允许配置主要规则参数



主要参数

您可以设定下列参数:

■程序路径. 单击浏览.并选择应用规则的应用程序 如果你想要的规则适用于所有的应用程序，选择任何.

- Command line （命令行）． 如果你想要的规则只应用于选定的应用程序是打开的并在Windows命令行界面具有特定命令的，清除 任何 复选框，在编辑领域键入相应的命令.
- 协议. 从菜单中选择规则应用的IP协议。
  - 如果你想要规则适用于所有协议，选择任何.
  - 如果你想要的规则适用于具体的协议，选择其他. 一个编辑窗口将会出现 在编辑窗口,给那些协议分配编号



注意

IP协议数字是被互联网编号分配机构（ IANA负责）编辑 你可以找到已分配的IP协议号码的完整名单www.iana.org/assignments/protocol-numbers.

- 事件. 根据选定的协议，选择应用于规则的网络事件。 下列事件可能考虑到:

事件	说明
连接	初步交换了标准信息所使用的面向连接的协议（如TCP ），以建立一个连接。 随着面向连接的协议，在连接建立之后的两台有数据通信的计算机之间。
通信	数据流通的两台计算机之间
注意	在这个状态里,有一个应用程序监控这个网络并等待来建立一个和同等的应用程序的连接,或从这个同等的应用程序接收信息

- 信任级别. 选择应用规则的信任等级
- 操作. 选择其中一个可用的行动:

操作	说明
允许	指定的申请将被允许网络/互联网接入，根据指定的情况下。
拒绝	指定的申请将被拒绝网/互联网接入，根据指定的情况下。

配置高级参数

高级配置窗口的标签允许配置高级规则参数





高级参数

您可以配置以下的高级参数:

■向导. 从菜单选择应用规则的通信向导

向导	说明
外出	规则只应用于发送的流量。
进入	规则只应用于接收的流量。
两者	规则对发送和接收的Cookie都生效。

■IP版本. 从菜单选择应用于规则的IP版本(IPv4，IPv6 或其他)

■源地址. 以下是特定的适用于规则的本地IP地址和端口

- 如果您有1个以上的网络适配器,你可以清除任何复选框并键入一个特定的IP地址。
- 如果你已经选择了TCP或UDP作为议定书您可以设置一个特定的港口或射程介于0和65535 。如果你想要使用规则适用于所有港口中, 选择 任何.

■远程地址. 以下是应用于规则的指定远程IP地址和端口:

- 要筛选您的计算机与特定的电脑之间的流量，清除任何复选框，键入其IP地址。
- 如果你已经选择了TCP或UDP作为议定书您可以设置一个特定的港口或射程介于0和65535 。如果你想要使用规则适用于所有港口中，选择 任何.

■应用这个规则只能直接连接到电脑上. 当您想要规则只应用于本地流量尝试,请选择此选项时

■检查原始事件的家长控制进程. 只有当您选择了 严格自动规则 时，您才可修改此参数（请到 设定 标签页并点击 高级设定）。 精密的规则意味着，当一个应用程序需要网络/互联网接入每次的家长进程是不同的.BitDefender将会提示您如何进行操作

20.3.4. 高级规则管理

如果你需要查看防火墙规则高级控制高级. 接着会显示一个新窗口。



高级规则管理

你可以根据防火墙规则所列出的顺序进行检查。 该表列提供每条规则的全面信息



注意

当一个连接开始尝试运作（无论是传入或传出）， BitDefender将用匹配一条规则应用于相应的连接运作。 因此，对其中的规则进行检查是非常重要的

要删除一个规则，请选中它并点击 删除规则 按钮。

要修改一个已有规则，请选中它并点击 编辑规则 按钮或者双击该规则。

你可以增加或减少的优先处理的规则。点击 上移进名单 按钮，增加一个层次优先选择，或点击 下移进名单 按钮，以减少一个层次优先选择。 转让规则的最高优先事项，请点击 先搬到按钮。转让规则最低优先，点击 最后移动 按钮。

点击 关闭 关闭窗口。

20.4. 连接控制

通过应用程序监测当前网络/互联网活动（TCP和UDP ） 并打开BitDefender防火墙日志，进入 防火墙活动 在高级浏览中。



连接控制

你可以看到全部的交通分类应用。每项申请的，你可以看到连接，以及开放口岸，以及统计方面卸任&来袭交通速度和总金额的数据发送/接收。

如果你也想看到不活动的程序,清除隐藏不活动的进程复选框。

该图标含义如下:

- 显示一个您的计算机上开放的连接
- 显示一个在您的计算机上加的开放端口。

窗口介绍了当前网络/网际网路活动，在实时性要求。作为连接或港口关闭，你可以看到相应的统计是暗淡的，并说，最终，他们消失。 同样的事情发生在所有数据相应的应用所产生的交通，或有个开放口岸，与你密切。

防火墙事件的记录名单（开启/禁用防火墙，通信阻断，修改设置）或因活动而生成的记录,并被这个模块发现（扫描端口，阻止连接尝试或交通根据规则）查看

BitDefender防火墙日志文件点击 显示日志. 该文件位于当前的Windows用户的文件夹中, 根据路径: BitDefender\BitDefender 防火墙\bd防火墙.txt.

如果你想让日志包含更多的信息,选择增加日志记录.



21. 加密

Bitdefender提供针对雅虎通和MSN的加密功能，保护您在聊天时不被窃取私密信息。

21.1. 即时通讯（IM）加密

默认情况下，如果满足下列条件，Bitdefender会加密您所有的聊天内容：

- 您的聊天对象装有支持即时通讯加密的Bitdefender产品，并且启用了针对该即时通讯软件的加密功能。
- 您和您的聊天伙伴使用雅虎通或MSN。



重要

如果您的聊天对象使用了网页聊天工具（如网页版雅虎通和MSN），或者其他支持雅虎通和MSN的软件，Bitdefender将不会加密聊天内容。

要设置即时通讯加密，请到高级视图中的 加密>即时通讯加密。



注意

您可以通过聊天窗口上的Bitdefender工具栏轻松设置即时通讯加密功能。 欲了解更多信息，请参阅 “集成到即时通讯软件” （第 51 页）。



BitDefender 全方位安全杀毒软件 - 试用版　切换至基本视图

状态：4 个等待处理的问题　修复

常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册

即时通讯加密　文件保险箱

即时通讯加密已禁用。
雅虎通加密已禁用。
MSN通信加密已禁用。

加密例外

用户 ID	即时通讯程序

当前连接

用户 ID	即时通讯程序	加密状态

您可在此配置即时通讯加密组件细节。

bitdefender　购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

即时通讯加密

默认情况下，启用针对雅虎通和MSN的即时通讯加密。 您可选择禁用针对某个聊天工具的加密或完全禁止此功能。

会显示两个列表：

■加密例外 – 列出禁用即时通讯加密的聊天联系人及对应聊天工具。 要从列表中删除一个联系人，请选中他然后点击 ⊟ 移除 按钮。

■当前连接 – 列出当前的即时通讯连接（用户名和聊天程序），以及是否启用加密。 以下原因会导致某些连接不被加密：

・您明确禁用对该联系人加密。

・您的联系人没有安装支持即时通讯加密的BitDefender版本。

21.1.1. 禁用对特定用户的加密

要禁用对特定用户的加密，请执行下列步骤：

1. 点击 添加 按钮打开设置窗口。



添加联系人

2. 在编辑框中输入联系人的用户账号。
3. 选择与该用户关联的即时通讯软件。
4. 点击 确定。

21.2. 档案库

BitDefender文件库让您可以创建加密，密码保护您计算机上的驱动器（或文件库），您可以安全地储存您的机密文件。 文件库的存储数据只有知道密码的用户能够使用。

密码允许你打开数据存储或关闭一个文件库，同时保持它的安全。 当文件库被打开，您可以添加新的文件，使用或更改当前文件。

本身,文件库就是一个在本地硬盘的文件存储具有的.bvd 虽然实际文件代表的文件库硬盘可以从一个不同的操作系统（如Linux ），信息存储在其中无法读取，因为它是加密的。

为了管理您的计算机上的文件库，进入加密文件库在高级浏览中。

BitDefender 全方位安全杀毒软件 - 试用版　切换至基本视图

状态：4 个等待处理的问题　修复

即时通讯加密　文件保险箱

常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册

☑ 文件保险箱已启用

此计算机上的保险箱

保险箱	状态	盘符	完整路径

保险箱内容

完整路径	文件类型

如需获知关于 BitDefender 用户界面各选项的详情，请移动您的鼠标并悬停于相应窗口。此区域将显示相关的帮助文本。

bitdefender　购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

档案库

如果要停用文件库，清除 文件库已启动 查看对话框并电击 是的 以确认。 如果您停用文件库,所有的文件库将被锁定，而您将不再能够再访问他们所包含的文件。

该表上方显示您的计算机上的文件库. 你可以看到的名称，状态（开/关），磁碟机代号和文件库的完整路径。 该表的底部显示选择的文件库的内容。

21.2.1. 创建一个文件库

要创建一个新的文件库，请使用这些方法:

■点击 创建文件保险箱。

■右键选择文件库列表并选择 创建.

■右击在您的计算机桌面上的或文件夹中的BitDefender文件库 并选择创建.

接着会显示一个新窗口。

BitDefender 2009 - 创建保险箱

磁盘上保险箱文件的完整路径(P)

浏览(B)...

盘符(L): K:

密码(P)

格式化驱动器(F)

确认(N)

密码的最短长度是 8 个字符。

保险箱大小(MB) 50

创建新的保险箱。

创建(R) 创建并打开(O) 取消(C)

创建文件库

以下步骤:

1. 指定的位置和名称的文件库文件。

   ■单击浏览.选择本地的文件库和保存自定义名字下面的库中文件

   ■在磁盘上标记文件库文件的完整路径。

2. 从菜单中选择一个硬盘的分区 当您打开文件库，一个被标记的虚拟磁盘驱动器选定的磁盘出现在我的电脑中。
3. 键入密码，在 密码栏。 试图打开文件库和访问它文件的任何人,必须先输入密码
4. 选择格式驱动器格式虚拟磁盘分配到文件库中
5. 如果您想更改文件库的默认大小（ 50 MB ），请键入所需的大小值文件库大小 .
6. 点击创建，如果您只想在选定的位置创建文件库。 在我的电脑中创建并显示文件库作为一个虚拟磁盘驱动器，单击创建打开.

21.2.2. 打开一个文件库

为了使一个文件库的文件存储开始工作，您必须打开文件库。 当您打开一个文件库，一个虚拟磁盘驱动器将会出现在我的电脑中 该驱动器是被标记的,驱动器分配给文件库。

打开一个文件库,你可以选择下列任何方法:

■从表中选择文件保险箱并点击 打开保险箱。

■桌面右键点击文件库并选择 打开.

■桌面右键点击文件库并选择BitDefender文件库 再单击 打开.

接着会显示一个新窗口。

BitDefender 2009 - 打开保险箱文件

磁盘上保险箱文件的完整路径(P)

E:\Data.bvd

盘符(L): G: 密码(P)

打开当前选定的保险箱。

打开(O) 取消(C)

打开文件库

以下步骤:

1. 从菜单中选择一个硬盘的分区
2. 键入密码, 在 密码栏。
3. 点击打开.

21.2.3. 锁定一个文件库

当你完成你在文件库的工作, 你必须锁定它, 以保护您的数据。

使用这些方法来锁定文件库:

■从表中选择文件保险箱并点击 锁上保险箱。

■右键点击桌面文件库,并选择 锁定.

■右键点击在您电脑上的文件库BitDefender文件库 并选择 锁定.

■从我的电脑中右键点击相应的虚拟磁盘驱动器BitDefender文件库 并选择锁定.

21.2.4. 更改文件库密码

要更改文件库密码,请用以下任何一种方法:

■从表中选择文件保险箱并点击 修改密码。

■右键点击文件库,选择 更改密码.

■右键点击您计算机上的文件库,进入BitDefender文件库 并选择改变文件库密码.

接着会显示一个新窗口。



更改文件库密码

以下步骤:

1. 键入原来的文件库密码, 原密码 。
2. 键入新的文件库密码在新密码 并 确认新密码.



注意

密码应该至少8字节长。 强密码是指组合了大写和小写字母、数字及特殊字符 (#、$ 和 @) 的密码。

3. 点击确认 修改密码。

21.2.5. 文件库添加文件

添加文件到文件库,完成这些步骤:

1. 点击 添加文件。 接着会显示一个新窗口。
2. 选择你想添加到文件库的文件/文件夹
3. 点击 好的 复制所选的对象进文件库。



注意
你不能把系统或应用程序文件添加到文件库.

21.2.6. 从文件库中删除文件

请跟随以下步骤来删除文件库中的文件:

1. 从文件库列表选择想删除的文件
2. 从列表中选择要被删除的文件,它将会显示文件的内容
3. 点击 × 移除文件。



注意
如果文件库是打开的,你可以从虚拟硬盘驱动分配的文件库中直接删除文件



22. 漏洞检测

要保证计算机不受黑客和恶意程序的侵害，一个非常重要的防范措施是保持您的操作系统和常用软件是最新版本。 此外，为防止对您计算机的非授权访问，必须为每个WIndows用户账户设置强密码（不能被轻易破解的密码）。

BitDefender定期检查您的系统漏洞，并通知您存在的问题。

22.1. 状态

要设置自动漏洞检测，或运行漏洞检测，请到高级视图中的 漏洞检测>状态。



漏洞检测状态

表中显示在上次漏洞检测中发现的问题及其状态。 如果有解决方案的话，您也能在表中看到。 如果操作是 无，则该问题不是一个漏洞。



重要
如要自动获得系统及应用程序漏洞的通知，请启用 自动检测漏洞。

22.1.1. 修补漏洞

要修复一个漏洞，请双击它，然后根据问题具体情况，按照下述说明操作：

- 如果有可用的Windwos更新，请点击 安装所有系统更新 进行安装。
- 如果应用程序已经过时，请使用 主页 链接下载并安装该程序的最新版本。
- 如果一个Windows用户帐户使用了弱密码，强制用户在下次登录时修改密码或直接帮用户修改密码。

你可以点击 立即检测 并按照向导指引修复漏洞。

步骤 1/6 – 选择要检测的漏洞



漏洞检测

点击 下一步 在系统中检查所选的漏洞。

步骤 2/6 – 检测漏洞



漏洞检测

请等待Bitdefender完成漏洞检测。

步骤 3/6 – 修改弱密码



用户密码

您可以看到您计算机上的Windows用户账户列表，以及每个账户的密码强度。点击 修复 修改弱密码。 接着会显示一个新窗口。

BitDefender
Choose method to fix:
Force user to change password at next login
Change user password
Type password:
Confirm password:
OK Close

修改密码

选择修复此问题的方法:

- 强制用户在下次登录时修改密码. Bitdefender会在用户下次登录Windows时提示用户更改密码。
- 更改用户密码. 您必须在编辑框输入新密码。



注意
强密码是指组合了大写和小写字母、数字及特殊字符（#、$ 和 @）的密码。

点击确认 修改密码。

点击 下一步。



步骤 4/6 – 更新应用程序



应用程序

您可看到BitDefender所检查的应用程序，以及它们是否最新版本。 如果应用程序不是最新版本，请点击后面的链接下载最新版本。

点击 下一步。

步骤 5/6 – 更新Windows



更新Windows

您可看到您的计算机上尚未安装的Windows关键及非关键更新列表。 点击 安装所有系统更新 要安装所有可用更新。

点击 下一步。



步骤 6/6 - 查看结果



查看结果

点击 关闭。

22.2. 设置

要设置自动漏洞检测，请到高级视图中的 漏洞检测>设置。



自动漏洞检测设置

选择您想定期检查的系统漏洞前面的复选框。

■Windows关键更新

■Windows常规更新

■弱密码。

■应用程序更新



注意

如果您清除了某类漏洞前的复选框，BitDefender将不会通知您相关问题。

23. 游戏/笔记本模式

游戏/笔记本模式模块可让您设置BitDefender的特殊运行模式:

■游戏模式　暂时修改产品设置以便在您玩游戏时将产品对系统资源的消耗降到最低。

■笔记本模式 在笔记本电脑使用电池时不运行计划任务，以延长电池使用时间。

23.1. 游戏模式

游戏模式暂时修改防护设置，以使产品对系统性能的影响最低。 在游戏模式下，会应用以下设置:

■所有Bitdefender警报和弹出窗口都被禁用。

■Bitdefender实时防护级别设置为 宽松。

■Bitdefender防火前设置成 允许所有. 这意味着所有新的连接（包括传入和传出）会自动允许，无论是端口和协议是否被使用。

■不进行升级。



注意

要更改此设置，请前往 升级>设置 并清除 在游戏模式下不进行升级 复选框。

■默认禁用任务计划。

默认情况下，当您运行一个BitDefender已知的游戏，或者某个应用程序全屏幕运行时，BitDefender会自动进入游戏模式。 您也可以使用默认热键 Ctrl+Alt+Shift+G 进入游戏模式。 强烈建议您在结束游戏后退出游戏模式（您可以使用相同的默认热键 Ctrl+Alt+Shift+G）。



注意

在游戏模式下，您可以看到字母 G 叠加在 BitDefender 系统托盘图标上。

要设置游戏模式，请到高级视图中的 游戏/笔记本模式>游戏模式。

游戏模式

在窗口的上方，您可看到游戏模式的状态。 您可以点击 进入游戏模式 或 退出游戏模式 改变当前状态。

23.1.1. 设置自动游戏模式

自动游戏模式允许BitDefender在检测到运行游戏时自动进入游戏模式。 您可以配置下列选项：

- 使用BitDefender内置的游戏列表 – 当您运行BitDefender列表中的已知游戏时自动进入游戏模式。 要查看此列表，请点击 管理游戏 然后点击查看允许的游戏。
- 于全屏时进入游戏模式 – 当应用程序全屏运行时， 自动进入游戏模式。



- 询问我是否将程序加入游戏列表 - 在离开全屏模式时，询问您是否将新应用程序加入游戏列表。 通过添加新的应用程序到游戏列表，下次启动它时BitDefender将自动进入游戏模式。



注意

如果您不希望BitDefender自动进入游戏模式，请清除 自动游戏模式 复选框。

23.1.2. 管理游戏列表

BitDefender在您运行游戏列表中的程序时会自动进入游戏模式。 要查看和管理游戏列表，请点击 管理游戏。 接着会显示一个新窗口。



游戏列表

以下情况下，新的应用程序会自动添加到列表中：

- 您启动了一个BitDefender已知游戏列表中的游戏。 要查看此列表，请点击 查看允许的游戏。
- 在离开全屏模式时，您从提示窗口将应用程序添加到了游戏列表。

如果您想对某个应用程序禁用自动游戏模式，请清除对应的复选框。 您应该对运行全屏模式的常用应用程序禁用自动游戏模式，比如浏览器和视频播放器。

要管理游戏列表，您可以使用表格上方的按钮：



- 添加 – 添加新的应用程序到游戏列表。
- 删除 – 从游戏列表中删除一个应用程序。
- 编辑 – 编辑游戏列表中的条目。

添加或修改游戏

当您向游戏列表中添加条目或编辑已有条目时，下面的窗口会出现：



添加游戏

点击 浏览 选择应用程序或输入该程序的全路径。

如果您不希望所选的程序启动时自动进入游戏模式，请选择 禁用。

点击 确认 将该条目加入游戏列表。

23.1.3. 配置游戏模式设置

要设置计划任务的特性，请使用下述选项：

- 扫描任务 – 禁止任务计划在游戏模式时运行。 您可以选择下列选项之一：

选项	说明
跳过任务	不要运行计划任务。
推迟执行任务	退出游戏模式后立即执行计划任务。

自动禁用BitDefender的防火墙，而在游戏模式下，按照下列步骤进行：

1. 点击 高级设置。 接着会显示一个新窗口。
2. 选择 不使用防火墙 复选框。
3. 点击 确定 保存修改。

23.1.4. 修改游戏模式热键

您也可以使用默认热键 Ctrl+Alt+Shift+G 进入游戏模式。 如果您想改变热键，请按照下列步骤：

1. 点击 高级设置。 接着会显示一个新窗口。



高级设置

2. 在使用热键选项下面，设置您希望使用的热键：

 ■通过选中下面的功能键来设置热键：Ctrl键Ctrl，Shift键Shift，Alt键Alt。

 ■在编辑框中输入您想使用的普通键。

 例如，如果您想使用 Ctrl+Alt+D热键，您需要选中 Ctrl 和 Alt 并输入 D。
3. 点击 确定 保存修改。



注意
清除 使用热键 旁的复选框将禁用热键。

23.2. 笔记本模式

笔记本模式是专为笔记本用户设计的，其目的是当笔记本靠电池供电时，使BitDefender对电池消耗降到最低。

在笔记本模式下，默认不运行计划任务。

BitDefender检测到您的笔记本切换到电池供电时会自动进入笔记本模式。 同样，BitDefender检测到您的笔记本不再用电池供电时会自动退出笔记本模式。

要设置笔记本模式，请到高级视图中的 游戏/笔记本模式>笔记本模式。



笔记本模式

您可看到笔记本模式是否启用。 如果笔记本模式已启用，BitDefender将在笔记本用电池供电时应用配置的选项。

23.2.1. 设置笔记本模式选项

要设置计划任务的特性，请使用下述选项：

■扫描任务 – 禁止计划任务在笔记本模式时运行。 您可以选择下列选项之一：

选项	说明
跳过任务	不要运行计划任务。
推迟执行任务	退出笔记本模式时立即运行计划任务。

24. 家庭网络

家庭网络模块可让您从一台计算机上管理你家里所有计算机上的Bitdefender产品。



家庭网络图

要管理安装在您家里各台计算机上的Bitdefender产品，请按照下列步骤进行：

1. 在您的计算机上加入Bitdefender家庭网络。 加入家庭网络需要为家庭网络管理设置一个管理员密码。
2. 将每台您希望管理的计算机加入家庭网络（设定密码）。
3. 回到您的计算机，并将所有你希望管理的计算机加入家庭网络。

24.1. 加入家庭网络

要加入家庭网络，请按照下列步骤进行：

1. 点击 加入/创建网络。 系统会提示您设置家庭网络管理密码。



设定密码

2. 请在两个编辑框输入相同的密码。
3. 点击 确定。

您将看到计算机名出现在家庭网络地图中。

24.2. 向家庭网络中添加计算机

在添加计算机到家庭网络之前，您必须为每台计算机配置Bitdefender家庭管理密码。

要添加计算机到bitdefender家庭网络，请按照下列步骤进行：

1. 点击 管理网络。 系统会提示您输入家庭网络管理密码。

BitDefender

您必须输入家庭管理密码。

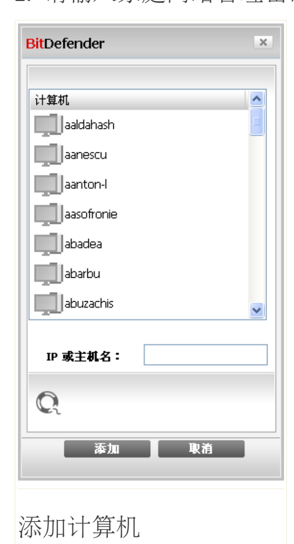
密码

本次操作期间不要再次显示此消息。

确定 取消

输入密码

2. 请输入家庭网络管理密码并点击 确定。 接着会显示一个新窗口。



添加计算机

您可看到家庭网络中所有计算机的列表。 图标含义如下:

■ 表示一台在线但是没有安装Bitdefender产品的电脑。

■ 表示一台在线并且安装了Bitdefender产品的电脑。

■ 表示一台离线的安装了Bitdefender产品的电脑。

3. 请执行如下操作之一:
   ■从列表中选择计算机名称加入。
   ■在对应区域输入要加入的计算机的IP地址或计算机名称。
4. 点击 添加。 系统会提示您输入该计算机的家庭网络管理密码。



权限验证

5. 输入在该计算机上设置的家庭网络管理密码。
6. 点击 确定。 如果您提供了正确的密码，选定计算机的名称会出现在家庭网络图中。



注意
您可以添加多达五台电脑到网络中。

24.3. 管理家庭网络

成功创建了Bitdefender家庭网络之后，您可以从一台计算机上管理所有计算机上的BitDefender产品。

BitDefender 全方位安全杀毒软件 - 试用版　切换至基本视图

状态：4 个等待处理的问题　修复

家庭网络

常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册

INTERNET
10.10.0.1
dflorea2-xp
此计算机
无 PC（点击添加）

注册此计算机（使用授权密钥）
设置配置密码
运行扫描任务
修复此计算机的问题
显示此计算机的历史记录
立即在此计算机上进行升级
应用方案
设置此计算机为网络中的升级服务器

添加计算机　离开网络　刷新

“家庭网络”模块将显示 BitDefender 家庭网络结构（若家庭网络尚未配置则以灰色显示）。请点击【加入/创建网络】以开始创建您的家庭网络。

bitdefender　购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

家庭网络图

移动鼠标光标到网络图中的一台计算机上，您可以看到该计算机的简要信息（名称、IP地址、影响系统安全的问题数、注册状态等）。

右键点击网络图中的一个计算机名，您会看到所有在该计算机上可以执行的管理任务。

■注册此计算机

■设置配置密码。

■运行扫描任务

■修复此计算机上的问题

■查看此计算机的历史记录

■立即在此计算机上运行升级

■应用策略

■在此计算机上运行系统优化

■将此计算机设置为本网络的升级服务器

在某台计算上运行任务之前，系统会提示您输入家庭网络管理密码。



输入密码

请输入家庭网络管理密码并点击 确定。



注意

如果您计划执行多项任务，您可选择本次操作期间不要再次显示此消息。 选择此选项，您在本次操作期间将将不会再次被提示输入密码。

25. 升级

每天都会发现新病毒，所以需要及时更新BitDefender病毒库。

如果您是通过宽带或DSL连接到互联网，BitDefender会自行处理升级事宜。默认情况下，产品在您启动计算机时检查更新，随后每 小时 进行一次检查。

如果发现了新升级包，可能会要求您确认进行升级，也可能自动进行升级，这取决于自动升级设置 里面的设置选项。

升级过程是逐步执行的，需要被更新的文件会被逐步替换，因此升级过程不会影响产品的正常运行，同时又可减少系统漏洞。

升级主要有以下几种类型:

- 反病毒引擎升级 – 随着新威胁的出现，病毒库也需要得到升级以防护最新病毒。这种升级类型也称作 病毒定义升级。
- 防垃圾邮件引擎更新 – 新规则将增加启发式和网址过滤器,并且新的图像将被添加到的图像过滤器。这将有助于提高反垃圾邮件引擎的效率。此更新类型也被称为防垃圾邮件更新.
- 反间谍软件引擎升级 – 新的间谍软件特征将被添加到数据库中，这种升级类型也称作 反间谍软件升级。
- 产品升级 – 当产品新版本发布时，会增加新功能和扫描技术以提升产品的性能。这种升级类型也称作 产品升级。

25.1. 自动升级

要查看升级相关的信息或进行升级，请到高级视图中的 升级>升级。



BitDefender 全方位安全杀毒软件 - 试用版 切换至基本视图

状态：4 个等待处理的问题 修复

升级 设置

常规
反病毒
反垃圾邮件
用户控制
隐私控制
防火墙
漏洞检测
加密
游戏/笔记本模式
家庭网络
升级
注册

自动升级已启用

上次检查 2009-1-19 16:23:17
上次升级 尚未进行
立即升级

病毒特征库属性

病毒特征库 2544627
引擎版本 7.23241
显示病毒列表

下载状态

升级已被取消，请停止运行中的扫描任务并重试。

文件： 0 % 0 KB
升级总进度 0 % 0 KB

请保持开启自动升级以确保BitDefender的病毒特征库始终保持最新版本。

bitdefender 购买/续订 - 我的账户 - 注册 - 帮助 - 技术支持 - 历史记录

自动升级

您可在此看到上次检查更新和上次执行升级的时间，以及上次升级执行时的信息（成功或发生错误）。此外，您还可看到当前引擎的版本以及病毒特征码数量。

如果您是在升级过程中打开此窗口，您还会看到下载的进度。



重要
要能不受最新病毒的侵害，请保持启用 自动升级。

点击 查看病毒列表 可以查看BitDefender的病毒特征码列表，您将看到一个包含所有特征码的HTML文件打开在浏览器中。您可点击 BitDefender病毒列表去BitDefender的在线特征码库搜索特定的病毒特征码。

25.1.1. 进行升级

任何时候您只需点击 立即升级 就可完成自动升级。这种升级方式也称作 用户请求的升级。

升级 模块会连接到BitDefender的升级服务器并检查是否有可用更新，如果发现了可用更新，则会根据在 手动升级设置 里的选择，提示您确认升级或者直接自动进行升级。



重要
升级完成后，可能有必要重新启动计算机。建议立刻重新启动。



注意
如果您通过拨号方式连接到网络，建议您定期手动升级产品。

25.1.2. 禁用自动升级

如果您禁用自动升级，会出现一个警告窗口。



禁用自动升级

您必须从列表中选择您想禁用自动升级多长时间以确认您的操作，您可禁用自动升级5分钟、15分钟、30分钟、1小时或直到下次系统重启。



警告
这是一个关键的安全问题。我们建议您禁用自动升级的时间越短越好。如果BitDefender不能定时升级，这将不能够保护您免受最新的威胁。

25.2. 升级设置

升级可通过本地网络、互联网进行，可直接连接或通过代理服务器连接。 默认情况下，BitDefender将每小时通过互联网检查更新，并安装可用的更新而不会进行提示。

要配置升级设置及管理代理服务器，请前往高级视图的 升级>设置。



升级设置

升级设置选项分为四个功能组（升级服务器设置，自动升级设置，手动升级设置 和 高级设置）。 以下将分别说明每个功能组。

25.2.1. 设置升级服务器

要设置升级服务器，请使用 升级服务器设置 部分的选项。



注意

仅当您是连接到存储了BitDefender病毒库的本地网络，或者通过代理服务器连接到互联网时，才需要设置这些选项。

要拥有更快速可靠的升级，您可以指定两个升级服务器：一个 首选升级服务器 和 一个 备选升级服务器。 默认情况下，两个升级服务器是相同的：http://upgrade.bitdefender.com。

要修改其中一个升级服务器，请在 URL编辑框中输入升级服务器的地址。



注意

建议您将首选升级服务器设置为本地服务器，而不更改备选升级服务器，作为在本地服务器出现故障时的容灾方案。

如果您的公司使用代理服务器连接到互联网，请选中 使用代理，然后点击 管理代理服务器 设置代理服务器选项。 欲了解更多信息，请参阅 “管理代理服务器”（第 264 页）

25.2.2. 设置自动升级

要设置让BitDefender自动执行升级，请使用 自动升级设置 中的选项。

您可以在 时间间隔 编辑栏指定两次更新检测的时间间隔。 默认情况下，更新时间间隔为1小时。

要指定自动升级过程如何进行，请选择下述选项之一：

- 静默升级 - BitDefender 将自动下载和安装更新。
- 下载升级包之前提示 - 每次发现可用升级包时，会提示您下载。
- 安装升级包之前提示 - 每次下载一个升级包之后，系统会在安装前提示您。

25.2.3. 手动升级设置

指定手动升级（用户请求的升级）如何执行，您可在 手动升级设置 组中指定一个选项：

- 静默升级 - 手动升级将自动在后台进行，无需用户干预。
- 下载升级包之前提示 - 每次发现可用升级包时，会提示您下载。

25.2.4. 设置高级设置选项

为防止 BitDefender 升级过程打扰您的工作，您可在 高级设置 组中设置相关的选项：

- 等待重启而不提示 - 如果升级后需要重启，产品会继续用旧文件运行，直到系统重启。用户不会被提示进行重启，用户的工作不会被打扰。
- 在进行扫描时禁止升级 - 在扫描进行时BitDefender将不会进行升级，这样升级进程不会干扰扫描任务。



注意

如果BitDefender在扫描进行时被升级，扫描过程将被中止。

- 游戏模式开启时禁止升级 - 在游戏模式时Bitdefender将不会进行升级。 这样，可以在游戏模式时将产品对系统性能的影响降到最低。

25.2.5. 管理代理服务器

如果您的公司使用代理服务器连接到互联网，您必须指定代理服务器设置，以便Bitdefender进行升级。否则，产品将使用安装产品的管理员的代理服务器设置，或者当前用户默认浏览器的服务器设置（如果可用的话）。



注意

只有具有系统管理员权限的用户或超级用户（知道产品配置密码的用户）才能修改代理服务器设置。

要修改代理服务器设置，请点击 管理代理服务器，会出现 代理服务器设置 窗口。



代理服务器设置

管理员的代理服务器设置（检测于安装时）

地址： 端口： 用户名称：

密码：

当前用户的代理服务器色绘制（检测自默认浏览器）

地址： 端口： 用户名称：

密码：

指定您的代理服务器设置

地址： 端口： 用户名称：

密码：

您可在此更改管理员的代理服务器设置。

确定 取消

代理服务器管理

代理服务器设置分为三组：

■管理员的代理服务器设置（检测于安装时） － 在安装时检测到的系统管理员的代理服务器设置，只有在您以系统管理员账户登录时才可设置。如果代理服务器需要用户名和密码，您必须在对应的编辑框中输入它们。

■当前用户的代理服务器设置（来自默认浏览器） － 从默认浏览器中获取的当前用户的代理服务器设置。如果代理服务器需要用户名和密码，您必须在对应的编辑框中指定。



注意

支持的浏览器为Internet Explorer、Mozilla Firefox 和 Opera。如果您使用其他浏览器，BitDefender 将无法获取当前用户的代理服务器设置。

■指定您的代理服务器设置 － 如果您以管理员身份登录，您可以指定自己的代理服务器设置。

需要指定如下设置选项：

・地址 － 输入代理服务器IP地址。



- 端口 – 输入代理服务器端口。
- 用户名 – 输入代理服务器用户名。
- 密码 – 请输入以上用户名的密码。

在试图连接到互联网时，BitDefender会尝试每一组代理服务器设置，直到连接成功。

首先会尝试您自己的代理服务器设置，如果连接不成功，则会尝试安装时检测的管理员代理服务器设置，如果还不能成功，则会尝试从默认浏览器中检测到的当前用户代理服务器设置。

点击 确定 保存修改并关闭窗口。

点击 应用 保存更改或点击 默认 加载默认设置。

26. 注册

要找到您的 BitDefender 产品的完整信息及注册状态，请到高级视图中的 注册。



注册

本部分显示:

■产品信息: BitDefender产品和版本。

■注册信息: 用来记录您的BitDefender账户信息的电子邮件地址(如果已经配置), 当前授权密钥及密钥过期时间。

26.1. 注册Bitdefender全方位安全杀毒软件

点击 立即注册 打开产品注册窗口。



注册

您可以看到Bitdefender注册状态，当前的授权密钥以及距离密钥过期所剩天数。

注册 Bitdefender 全方位安全杀毒软件

1. 选择我想要使用新的密钥注册产品。
2. 在编辑框中输入授权密钥。



注意
您可以找到您的授权密钥:
■在光盘标签上。
■在产品注册卡上。
■在网上购买的电子邮件中。

如果您没有Bitdefender授权密钥，请点击产品中所提供的链接前往Bitdefender网站购买。

点击完成。



26.2. 创建一个BitDefender账户

作为注册过程的一部分，您必须创建一个BitDefender账户。 该BitDefender账户可让您获得BitDefender升级、免费技术支持和特别促销活动。 如果您丢失了您的Bitdefender授权密钥，您可以登录到您的账户重新获取它，登录网址为 http://myaccount.bitdefender.com。



重要

您必须在安装BitDefender后15天内创建一个账户（如果您已注册产品，截止日期延长至30天）。 否则， BitDefender将不再更新。

如果您尚未创建BitDefender账户，请点击 创建一个帐户 打开帐户注册窗口。



创建账户

如果您此时不想创建Bitdefender账户，请选择跳过注册 并点击完成。 否则，根据您当前的情况继续进行：

- “我没有BitDefender账户” （第 270 页）
- “我已经有一个BitDefender账户” （第 270 页）

我没有BitDefender账户

要创建BitDefender账户，请选择 新建Bitdefender账户并提供所需的信息。 您在这里提供的信息都将保密。

- 电子邮件地址– 输入您的电子邮件地址。
- 密码 – 输入您Bitdefender账户的密码。 密码不得少于6个字符。
- 再次输入密码 – 请输入先前输入的密码。
- 名字 – 您的名字。
- 姓– 您的姓。
- 国家 – 选择您居住的国家。



注意
使用您提供的电子邮件地址和密码登录您的账户：http://myaccount.bitdefender.com。

要成功建立账户，您必须先激活您的邮件地址。请检查您的邮件地址，并按照BitDefender注册服务系统发给您的邮件里的说明进行。

Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。 选择一个可用选项：

- 请给我发送所有来自BitDefender的邮件
- 仅发送重要消息
- 不要给我发送任何消息

点击完成。

我已经有一个BitDefender账户

Bitdefender会自动检测你这台计算机以前是否注册过Bitdefender账户。 在这种情况下，请输入您账户的密码。

如果您已经有一个正常账户，但是Bitdefender没有检测到，请选择登录已存在的Bitdefender账户 并输入您账户的电子邮件地址和密码。

如果您忘记了密码，请点击忘记密码?然后按照说明进行。

Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。 选择一个可用选项：

■请给我发送所有来自BitDefender的邮件
■仅发送重要消息
■不要给我发送任何消息

点击完成。

获得帮助



27. 技术支持

做为一个增值服务提供商，BitDefender致力于为我们的用户提供卓越快速的支持。用户支持中心（您可在下面看到联系方式）会始终保持对最新威胁的敏锐了解，您可在此获得及时的支持服务。

BitDefender始终将用合理的价格为用户提供领先的产品做为自己的信念，此外，我们相信程序的业务建立在和客户的良好沟通以及卓越的客户服务之上。

我们欢迎您的咨询，请将您的问题发至 support@bitdefender.com。为了帮助我们能够快速地解决您的问题，请在电子邮件中尽可能多地提供您的问题详情，您的系统配置以及问题的准确描述。

27.1. BitDefender知识库

BitDefender 知识库是BitDefender产品有关信息的在线仓库。您也可以在此轻易地找寻您提出的问题的解决方案。报告是由BitDefender 的支持及开发组提供。它们也同时提供了一些有关反病毒防范措施的文章，BitDefender 管理组的方案和解说以及更多的有趣的文章。

BitDefender知识库是公开的，客户可以通过它进一步地了解病毒，增进对电脑病毒的知识。客户所发来的有效病毒报告以及咨询都即将列入BitDefender 知识库中。

您可以随时在此网址阅读BitDefender知识库 http://kb.bitdefender.com。

27.2. 请求帮助

27.2.1. 网上自助服务

有问题？我们的安全专家将通过电话、电子邮件或即时聊天为您提供免费的 7x24小时支持。

请点击如下链接：

英语

http://www.bitdefender.com/site/KnowledgeBase/

德语

http://www.bitdefender.com/de/KnowledgeBase/

法语

http://www.bitdefender.com/fr/KnowledgeBase/

罗马尼亚语

http://www.bitdefender.com/ro/KnowledgeBase/

西班牙语

http://www.bitdefender.com/es/KnowledgeBase/

27.2.2. 开始一个支持令牌

如果您想开始一个支持令牌，并通过电子邮件收到支持信息，请点击如下的链接之一：

英语：http://www.bitdefender.com/site/Main/contact/1/
德语：http://www.bitdefender.de/site/Main/contact/1/
法语：http://www.bitdefender.fr/site/Main/contact/1/
罗马尼亚语：http://www.bitdefender.ro/site/Main/contact/1/
西班牙语：http://www.bitdefender.es/site/Main/contact/1/

27.3. 联系信息:

我们相信高效的沟通是业务成功的关键，十年以来，BitDefender 已经建立起了一套超出用户期望的沟通体系。如果您有任何问题，请随时联系我们。

27.3.1. 网址

销售部：sales@bitdefender.com
技术支持：support@bitdefender.com
文档：documentation@bitdefender.com
合作伙伴项目：partners@bitdefender.com

市场部: marketing@bitdefender.com
媒体关系: pr@bitdefender.com
工作机会: jobs@bitdefender.com
提交病毒: virus_submission@bitdefender.com
提交垃圾邮件: spam_submission@bitdefender.com
报告不当使用: abuse@bitdefender.com
产品网址: http://www.bitdefender.com
产品FTP存档: ftp://ftp.bitdefender.com/pub
各地代理商: http://www.bitdefender.com/partner_list
BitDefender知识库: http://kb.bitdefender.com

27.3.2. 分公司

BitDefender的分公司都非常乐意在它们的业务区回答您的任何咨询，以下是它们的地址以及电话号码。

美国

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
电话: 1-954-776-6262
网站: http://www.bitdefender.com

技术支持（仅注册用户）:
- 电子邮件: support@bitdefender.com
- 电话（免费）:
  - 美国: 1-888-868-1873
  - 加拿大: 1-866-947-1873

客户服务(仅注册用户可用):
- 电子邮件: customerservice@bitdefender.com
- 电话（免费）:
  - 美国: 1-888-868-1873
  - 加拿大: 1-866-947-1873

德国

BitDefender GmbH

机场办事处中心
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Hotline: +49 2301 91 84 555
Technische Beratung: support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Web: http://www.bitdefender.de

英国和爱尔兰

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
电话: +44 (0) 8451-305096
电子邮件: info@bitdefender.com
销售: sales@bitdefender.com
网站: http://www.bitdefender.co.uk
技术支持: support@bitdefender.com

西班牙

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: soporte@bitdefender-es.com
Ventas: comercial@bitdefender-es.com
Phone:+34 932189615
Fax:+34 932179128
Sitio web del producto: http://www.bitdefender-es.com

罗马尼亚

BITDEFENDER
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
技术支持: support@bitdefender.com
销售: sales@bitdefender.com
Tel.: +40 21 3001226; +40 21 3001227; +40 21 3001228; +40 21 3001229

Fax: +40 21 2641799
产品网址: http://www.bitdefender.com

BitDefender救援光盘

28. 概览

BitDefender全方位安全杀毒软件带有一个可引导光碟（bitdefender光盘版），在您的系统启动之前,能够扫描并消毒所有现存的硬盘驱动器病毒.

若您的操作系统因为感染病毒无法正常操作，请用BitDefender 救援光碟。通常这是因为您没有使用反病毒产品导致。

每次启动BitDefender救援光盘时，病毒库会自动升级，无需用户干预。

BitDefender 救援光盘是由BitDefender改造的Knoppix发行版，集成了最新的BitDefender Linux 安全解决方案到 GNU/Linux Knoppix 光盘，可以扫描并清楚硬盘上（包括Windows NTFS分区）的病毒。此外，在您无法启动 Windows时，您还可用BitDefender救援光盘恢复重要数据。



注意
Bitdefender救援光盘可以在以下地址下载：http://download.bitdefender.com/rescue_cd/

28.1. 系统需求

启动BitDefender救援光盘之前， 您必须确保您的系统符合以下的需求:

处理器类型
: x86兼容处理器，主频不小于 166 MHz。如果是800MHz的i686级别处理器，会有更好的性能。

内存
: 内存至少为512MB(推荐1G)。

光驱
: BitDefender 救援光盘需要从光盘运行，因此必须有光驱，并且BIOS可以从光盘启动。

网络连接
: 虽然 BitDefender 救援光盘运行并不需要互联网连接，但是升级过程需要可用的HTTP连接，即便是通过代理服务器。因此，要获得最新的防护能力，必须有互联网连接。

图形分辨率
: 标准包括SVGA兼容图形卡。

28.2. 含有的软件

BitDefender 救援光盘 (Rescue CD) 含有以下软件:

Xedit
: 这是一个文本文件编辑器。

Vim
: 是一个功能强大的文本文件编辑器，包含语法高亮，图形界面以及更多其他功能。如需更多信息，请参阅 Vim homepage。

Xcalc
: 这是一个计算器。

RoxFiler
: Roxfiler是一个快速和强大的图形文件管理器。

  如需更多资讯，请参阅 RoxFiler homepage。

MidnightCommander
: GNU Midnight Commander (mc) 是一种文本模式文件管理器。

  如需更多资讯，请参阅 MC homepage。

Pstree
: Pstree显示正在运行的进程。

Top
: TOP 显示Linux的任务。

Xkill
: Xkill关闭一个客户端的 X资源。

Partition Image
: 分区映像帮您将分区存储为 EXT2、Reiserfs、NTFS、HPFS、FAT16 及 FAT32 文件系统的映像文件。此程序可用于备份。

  如需更多资讯，请参阅 Partimage homepage。

GtkRecover
: GtkRecover 是一个基于GTK版的控制台程序恢复，它可以帮助你恢复一个文件。

  如需更多资讯，请参阅 GtkRecover homepage。

ChkRootKit
: ChkRootkit是一个帮您扫描计算机上 rootkit 的工具。



如需更多资讯，请参阅 ChkRootKit homepage。

Nessus Network Scanner

Nessus是一个用于Linux、Solaris、FreeBSD及Mac OS X上的远程安全扫描器。

如需更多资讯，请参阅 Nessus homepage。

Iptraf

Iptraf是一个IP网络监控软件。

如需更多资讯，请参阅 Iptraf homepage。

Iftop

Iftop 显示带宽利用情况。

如需更多资讯，请参阅 Iftop homepage。

MTR

MTR是一个网络诊断工具。

如需更多资讯，请参阅 MTR homepage。

PPPStatus

PPPStatus 显示收到和发出的 TCP/IP 流量统计信息。

欲了解更多信息 请查阅 PPPStatus homepage。

Wavemon

Wavemon 是一个监控无线网络设备的应用程序。

欲了解更多信息，请查阅 Wavemon homepage。

USBView

USBView 显示连接到 USB 总线的设备信息。

欲了解更多信息，请查阅 USBView homepage。

Pppconfig

Pppconfig 帮您自动设置拨号ppp连接。

DSL/PPPoe

DSL/PPPoe 配置 PPPoE（ADSL）连接。

I810rotate

I810rotate 使用 i810switch(1)切换i810上的视频输出。

欲了解更多信息，请查阅 I810rotate homepage。



Mutt
Mutt 是一个功能强大的基于文本的 MIME 邮件客户端。

更多信息请查阅 Mutt homepage。

Mozilla Firefox
Mozilla Firefox 是著名的网页浏览器。

更多信息请查阅 Mozilla Firefox homepage。

Elinks
Elinks 是一个文字模式的网页浏览器。

更多信息请查阅 Elinks homepage。

29. BitDefender救援光盘使用说明

本章柏涵如果启动及停止 BitDefender 救援光盘、如何扫描计算机以及如何从被感染的计算机上将数据保存到移动设备上的信息。此外，利用光盘上提供的程序，您还可以做更多事情。

29.1. 启动BitDefender救援光盘

要启动光盘，首先设置您计算机的BIOS从光盘启动，然后将光盘放入光驱并重启系统。请确认您的计算机可以从光盘启动。

等待下一个屏幕出现，再根据屏幕上的指示来启动 BitDefender救援光盘。



注意
从列表中选择您想使用的语言。

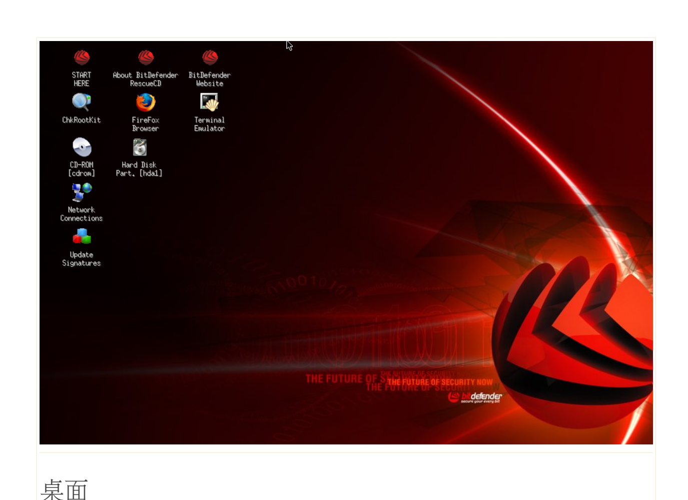


启动屏幕

启动时会自动升级病毒库，这可能需要一些时间。

当启动进程完成后，您将会看到桌面屏幕，此时可以使用 BitDefender 救援光盘。

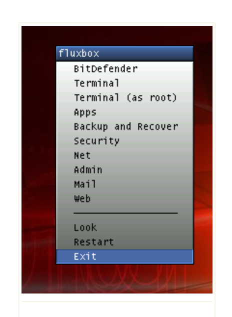




桌面

29.2. 停止BitDefender救援光盘

要安全地关闭您的电脑，请选择BitDefender救援光盘右键菜单上的 退出，或在终端上执行 halt 命令。



选择 “退出”

在 BitDefender 救援光盘成功关闭所有程序后，就会显示一个如下的屏幕。此时可以取出光盘以便从硬盘启动。现在您可以关闭计算机并重启。

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksusper
) (aio/0) Done.
Waiting for processes to finish.....................................
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd) (
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....................................
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/ini
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes]._
```

当关闭时，请等待这一信息

29.3. 如何进行反病毒扫描?

在启动进程结束后，会显示一个向导程序，此时可以全面扫描您的计算机。您只需点击 Start 按钮即可。



注意
如果你的屏幕分辨率不够高，您将会被要求在文本模式下进行扫描。

请遵循向导程序的三个步骤来完成扫描过程。

1. 您可以看到扫描的状态和统计信息（扫描速度、已用时间、扫描/感染/可疑/隐藏对象的数目等）。

   注意
   扫描过程可能需要较长时间，取决于扫描的复杂程度。

2. 您可看到影响您计算机的问题数。

   这些问题被分组显示。 点击"+"的以展开一个组或点击 “-” 的格子以收起一个组。

   您可为每个问题组选择一个整体的操作，或者为每个问题选择单独的操作。

3. 您可看到扫描结果的摘要。

如果您要扫描某个目录，请按如下方式操作：

浏览您的文件夹，右键点击一个文件或目录并选中 发送到（Send to）。然后选择BitDefender扫描器（BitDefender Scanner）。

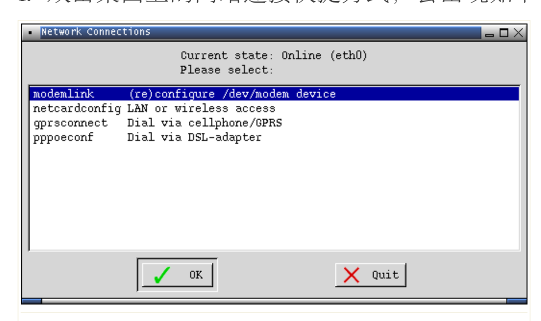
您也可以 root 身份在一个终端上发出如下命令。BitDefender反病毒扫描器（BitDefender Antivirus Scanner）将把选中的文件或文件夹当作默认的对象进行扫描。

```
# bdscan /path/to/scan/
```

29.4. 如何设置互联网连接？

如果您是在的动态主机配置学医（DHCP）网络中，并拥有以太网网卡，互联网连接会被自动检测及配置。如果想手工配置，请参照如下步骤。

1. 双击桌面上的网络连接快捷方式，会出现如下窗口。



网络连接

2. 选择连接类型并单击确定。

连接	说明
modemlink	当您使用调制解调器和电话线上网时，选择这种类型的连接。

连接	说明
netcardconfig	如果您使用局域网 (LAN) 接入互联网时，请选择这种类型的连接。这也适用于无线连接。
gprsconnect	当年使用移动电话GPRS连接到互联网时，请选择这种类型的连接。
pppoeconf	当您使用 DSL 调制解调器连接到互联网时，请选择这种类型的连接。

3. 请根据屏幕上的指示操作，如果您不确定要写什么，请联系您的系统管理员或网络管理员。



重要
请注意，您只能通过选择上述的选项才能启动调制解调器。要配置网络连接请参照下述步骤。

1. 右键单击桌面，Bitdefender救援光盘的右键菜单将会出现。
2. 选择Terminal(as root)。
3. 输入以下命令：

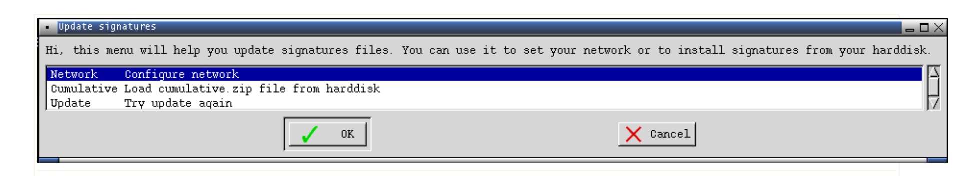
```
# pppconfig
```

4. 请根据屏幕上的指示操作，如果您不确定要写什么，请联系您的系统管理员或网络管理员。

29.5. 如何升级BitDefender?

启动时会自动升级病毒库，但是如果您跳过了此步骤，请参照如下说明升级BitDefender。

1. 双击桌面上的 Update Signatures 快捷方式，会显示如下窗口。



升级病毒库

2. 请执行如下操作之一:
   ■选择 Cumulative 安装已经保存在您硬盘上的病毒库，可以通过浏览您的计算机并加载 cumulative.zip 文件来实现。
   ■选择 Update 立即连接到互联网并下载最新的病毒库。
3. 点击 确定。

29.5.1. 如何通过代理服务器升级Bitdefender?

如果在您的计算机和互联网之间有代理服务器，需要进行一些设置以升级病毒库。

要通过代理服务器升级 Bitdefender，请参照如下步骤:

1. 右键单击桌面，Bitdefender救援光盘的右键菜单将会出现。
2. 选择Terminal(as root)。
3. 输入命令: cd /ramdisk/BitDefender-scanner/etc。
4. 输入命令: mcedit bdscan.conf 使用 GNU Midnight Commander来编辑文件。
5. 取消注释以下行: #HttpProxy = (仅删除 # 符号) 并指定代理服务器的域名、用户名、密码及服务器端口。例如，各行应和下面的例子近似:

   HttpProxy = myuser:mypassword@proxy.company.com:8080
6. 按 F2 保存当前文件，确认保存，按F10 关闭文件。
7. 输入命令: bdscan update。

29.6. 如何保存我的数据?

假设您因为某些原因不能启动您的Windows计算机，同时您需要访问计算机上的一些重要数据，此时可以使用 BitDefender 救援光盘来帮您。

要将数据从计算机上保存到移动设备中（如U盘），请参照如下步骤:

1. 把Bitdefender救援光盘放到光驱中，把U盘放入 USB 驱动器中，然后重启计算机。



注意

如果您想稍后插入U盘，请按照如下步骤安装移动设备：

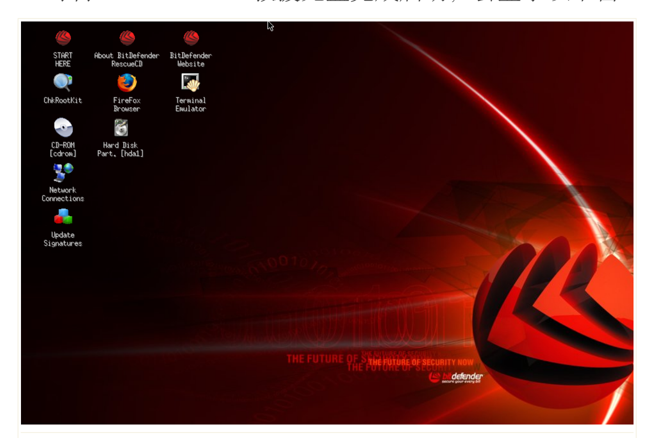
a. 双击桌面上的终端仿真程序（Terminal Emulator ）。

b. 输入下面的命令：

```
# mount /media/sdb1
```

请注意，根据您的计算机配置，可能是 sda1 而不是 sdb1 。

2. 等待 BitDefender 救援光盘完成启动，会显示以下窗口：



桌面

3. 双击数据所在的分区（例如 [sda3]）。



注意

当使用Bitdefender救援光盘时，您会处理的Linux型分区名。所以 [sda1] 可能会对应到Windows的（C:）分区，而 [sda3] 对应（F:）， [sdb1] 对应U盘。



重要

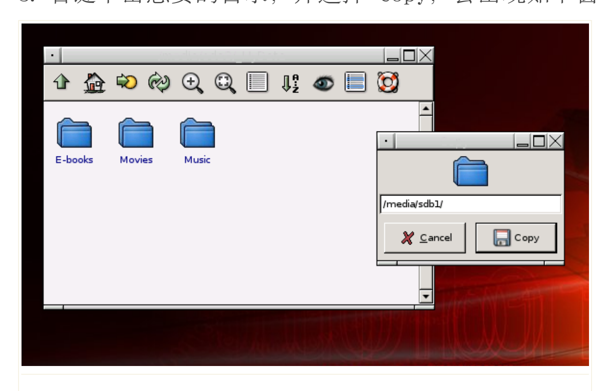
如果您的电脑没有正确关闭，可能会有某些分区没有自动安装。要装入一个分区，请按照下列步骤。

a. 双击桌面上的终端仿真程序（Terminal Emulator ）。

b. 输入下面的命令：

```
# mount  /media/partition_name
```

4. 浏览你的文件夹，并打开想要的目录。例如，MyData目录，它包含 Movies、Music 和电子图书 子目录。
5. 右键单击想要的目录，并选择 Copy，会出现如下窗口。



保存数据

6. 输入 /media/sdb1/ 到相应的文本框，然后点击Copy。

   请注意，根据您的计算机配置，可能是 sda1 而不是 sdb1 。

词汇表

ActiveX

ActiveX 是一种写程序的模型，因此其他的程序和操作系统可以调用它。ActiveX 技术被用于和 Microsoft Internet Explorer浏览器一起使用，来创建和计算机程序类似的交互型网页。使用ActiveX，用户可以提问或回答问题、使用按钮并可和网页用其他方式交互。ActiveX控件通常使用 Visual Basic 编写。

值得注意的是Active X 完全缺少安全控制；计算机安全专家不建议在网络中使用它。

Adware（广告软件）

Adware（广告软件）一般是跟免费的宿主应用程序一起的，只要用户同意并接受Adware（广告软件）。因为Adware（广告软件）应用程序一般是在用户同意了一个说明了程序目的的授权使用协议之后才进行安装，因此并不算冒犯用户。

但是，弹出的广告可能非常恼人，有时甚至影响系统性能。此外，某些此类程序收集的信息可能侵犯用户隐私。

归档文件（压缩包）

含有已经被备份文件的磁盘，磁带或是目录。

它是一个含有一个或多个文件的压缩文件。

Backdoor （后门）

它是一个设计者或维修者故意留下的系统安全的漏洞。这样的漏洞的动机不一定总是恶意的，例如，有的操作系统在出厂时就留有给技术支持人员或维护人员留的特权账户。

Boot sector（引导扇区）

它是一个在每一个磁盘的头部的扇区，用以说明磁盘的体系结构（扇区大小，簇大小等等）。为了引导磁盘，引导扇区还包含载入操作系统的一段程序。

Boot virus（引导扇区病毒）

它是一个可以感染硬盘或软盘引导扇区的病毒。如果尝试从被引导扇区病毒感染的磁盘启动，那么将会导致此病毒在内存里活动。从这时起，当每次您启动您的系统时，病毒将会在内存里活动。

浏览器

它是网络浏览器的简称。它是一个用作查找和显示网络网页的应用程序。两个最受欢迎的浏览器是：Netscape Navigator和微软Internet Explorer）。这两个浏览器都是图形界面，也就是说它们可以显示图像和文字。另外，现代多数



的浏览器可以显示多媒体信息，包括声音和视频，虽然它们需要一些格式的插件。

Command line （命令行）

在命令行界面下，用户使用命令行语言在屏幕上直接输入命令。

Cookie

在互联网行业，Cookies是指您计算机上包含可被广告商用来追踪您的兴趣和爱好的信息的小文件。Cookie技术仍处于不断发展中，其目的是直接向您展示您感兴趣的广告。不过对很多人来说，这是一把双刃剑。一方面，您可有效地看到符合您兴趣的广告，另一方面，Cookie会跟踪并记录您访问了什么网页以及点击了什么地方。可以理解，会有有关隐私的争论，而且很多用户觉得Cookie被用作类似“条形码”的用途而感觉被冒犯。虽然此观点可能有点极端，但在某些情况下的确如此。

Disk drive （磁盘驱动器）

这是一个从磁盘上读写数据的设备。

硬盘驱动器可在硬盘上读写数据。

软盘驱动器可在软盘上读写数据。

磁盘驱动器可以是内置的（在计算机内部），也可以是外置的（连接到计算机上的外置设备）。

Download （下载）

从源主机往外围设备复制数据（通常是一个文件）的过程，此术语通常用来描述从在线服务向个人计算机复制文件的过程。此外，下载还可以指从网络文件服务器向网络中的计算机复制文件的过程。

E-mail （电子邮件）

Electronic mail的缩写。一种通过局域网或广域网在计算机上发送消息的服务。

事件

由程序检测到的操作或发生的事情。事件可能是用户操作，例如点击鼠标按钮或按下键盘等，也可能是系统中发生的事情，如内存溢出。

False positive （误报）

是指扫描程序将正常文件认定为受感染的文件。

Filename extension （文件扩展名）

它是文件名句号后的部分，表示文件类型。

许多操作系统（比如Unix，VMS，和MS-DOS）都用文件扩展名，它通常在一到三个字母之间。例如C源程序的“c”，PostScript语言的"ps"，文本文件的"txt"。

Heuristic（启发式）

它是一个用来检测新病毒的基于规则的方法。该方式的扫描不需要依靠病毒库。启发式扫描的好处是不会被现存病毒的变种所欺骗。但是，它有可能报告一个正常程序中含有可疑代码，从而导致所谓的“误报” （"false positive"）。

网际网络协议

网际网络协议（Internet Protocol） – 在TCP/IP 协议组里的一个路由协议，主要处理IP寻址、路由、分解及组装IP包。

Java applet（Java 小程序）

它是一个只在网页上运行的Java程序。为了要在网页上用Java 小程序，您需要指明这个Java 小程序的名字和Java 小程序可以利用的大小（长和宽，以像素为单位）。当一个含有Java 小程序的网页被访问时，浏览器会从服务器下载其Java 小程序并在客户端上运行。Java 小程序和应用程序不同，它被一个严格的安全协议所管理。

例如，尽管Java 小程序是在客户端上运行，但是它不可以读写客户端计算机。另外，小程序被进一步的约束着，所以它只可以在它所来自域名里进行数据读写。

Macro virus （宏病毒）

一种以宏命令方式嵌入文档中的电脑病毒，许多应用程序，如 Word 和 Excel，支持强大的宏语言。

这些程序允许在文档中嵌入宏，每次打开文档就将执行宏。

Mail client （电子邮件应用程序）

电子邮件应用程序使用户可以编写、接收和发送邮件。

内存

计算机的内部存储区域，术语“内存”指以芯片方式存放的数据，“存储”是指存在于磁带或磁盘上的内存。每台计算机都带有一定数量的物理内存，通常被称为主存或 RAM。

Non-heuristic(非启发式)

这种扫描方式依赖病毒特征库，其优点是不会被看起来像是病毒的文件欺骗，因此很少产生误报。

Packed programs （加壳程序）

压缩后的文件。许多操作系统和应用程序都有可以压缩文件的指令以便减少内存使用。比如，一个文本文件包含10个连续的空格字符，通常就会需要10个字节存储。

但是，一个压缩程序会将空格字符替换为一个特殊的空格序列字符，然后跟上被替换的空格数。这样，10个空格字符只需两个字节存储。这只是一种加壳方式，还有很多其他的加壳方式。

路径

指打开系统内一个文件或文档的路径。通常，文档是从最高等级的开始分等级地分类。或指两个终点之间的路径，比如两台计算机之间的路径。

网络中任意两个网点之间的一段路由。在数据库中,从根段到个别段之间的段(具体)值序列。在IBM的通信系统ACF/VTAM中,连接终端和主处理机中应用程序的中间网点和数据链路。在IBM系统网络体系结构(SNA)中,两个网络的可寻址单元(NAU)之间 交换的信息所经过的一系列通路控制网络成分(路径控制程序和数据链路控制程序)。通路由 虚拟路由及其扩充路由(如果有的话)所组成。

Phishing （钓鱼）

网上欺骗的一种方式。骗子伪装成合法公司的职员发送电子邮件给目标，意图要目标公开自己的个人资料，在用此资料进行偷窃。电子邮件会将目标连往一个网站，便要求目标输入合法公司已经拥有的各人资料（比如密码，信用卡，身份证号码和银行户口号码），可网站是欺骗的工具。

Polymorphic virus （多形病毒）

可以侵略系统也同时可以变形的电脑病毒。这些病毒没有一定的二元图，也因此非常难查到。

端口

可以连接器材的端口。私人计算机共有几种端口。系统内部已有可连接硬盘，银幕和键盘的端口。系统外部又有可连接调制解调器，打印机，鼠标以及其他器材的端口。在TCP/IP和UDP网络内的终点，端口号数能指定用什么端口。

比如说，端口80是HTTP（WWW服务程序所用的协议）所用。在计算技术和通信技术中,网点上的一种功能部件,通过它数据可进入或离开一个数据网络或计算机。数据进出某功能部件的一种接口。

Report file （报告文件）

此文件列出已运用过的措施。BitDefender 保存着一个含有扫描过的路径，文件夹，存档和文件资料，以及受感染和可以文件的报告文件。

Rootkit程序

Rootkit是一系列提供系统管理的软件工具.这个名词首先是在UNIX操作系统中出现的,指提供入侵管理权的编译工具,他们能隐藏自己不被系统管理员发现.

Rootkits 的主要作用是隐藏进程、文件、登录信息或日志，同时，如果正当的软件用于不正当的目的，它们也可从终端、网络连接或外设拦截数据。

Rootkits 本质上不具有恶意目的。例如，系统甚至某些应用程序会隐藏所使用的关键文件。然而，它经常用于隐藏恶意软件或系统闯入者的出现。当与恶意软件结合在一起时，Rootkits构成了对系统完整性和安全的最大威胁。它们可以监控流量、创建系统的后门，更改文件以及日志以避免被发现。

脚本

是宏或批量处理文件的另外一种名称。运用脚本不需用户者指令。

垃圾邮件

电子垃圾邮件或新闻组的垃圾新闻。一般它是指任何的未经过用户者同意就发送的邮件。

Spyware（间谍软件）

它是一种擅自通过网络联系累积用户者资料的软件。通常用于传送广告。它们通常潜入可从网上下载的免费或共享软件；不过大多数的免费或共享软件都不藏间谍软件。安装后，间谍软件会通过用户的网络联系把资料暗中传送出去。

这些软件有取得电子邮址，密码和信用卡号码的能力。间谍软件与木马相似的是用户都是在不知道的情况下安装它们的。

下载和安装对等的(peer-to-peer/p2p)软件是非常容易受间谍软件侵入的方式。除了采用不道德的方式偷取个人资料以外，间谍软件也会使用户的系统缓慢，使用系统的内存和网络联系宽带，长期内会使用户系统运行不顺畅，甚至是系统崩溃。

Startup items （开始项目）

在这文件夹内的任何文件都会在系统起动时起动。起动时的银幕，音响效果，日志或任何应用程序都能成为起动物。通常在此文件夹内的文件都是别名文件。

系统栏

和视窗95同时推出，在视窗任务栏内的系统任务栏（通常在系统时钟旁）。它含有小型图形让用户轻易运用系统功能（比如传真，打印机，调制解调器，声量等）。双击任何图形可打开功能选项和详情。

TCP/IP

传输控制/互联网协议。用于不同操作系统，体系结构的网络基本协议。它定下了计算机之间的联络协议和条例，是互联网以及许多网络的通讯基础之一。

Trojan （木马）

伪装为良性程序的危险应用程序。此病毒种类并不会繁殖，但一样有危害性。最普遍的木马常伪装为反病毒软件，但其实是木马病毒。

一般此种病毒分成服务器端和客户端两部分，如计算机网络中服务器端被此程序感染，别人可通过网络其它计算机任意控制此计算机，并获得重要文件。国内流行的此类病毒有BO、NETSPY等。

升级

取代旧版本的新版本软件。另外，安装更新时，系统通常会确定旧版本已安装在系统内否则无法继续更新。

BitDefender拥有自己的更新模块让您指定或自动更新软件。

Virus （电脑病毒）

在您不知道的情况下存入系统并且启动的程序。多数的电脑病毒都能繁殖。所有的电脑病毒都是人造的。要创建一个会自己繁殖的电脑病毒并非一件难事。就连这样的简单病毒都有一定的危害性。它能够用尽系统的内存，使系统进入暂停的状态。更恶劣的病毒有通过网络联系以及保安措施的能力。计算机病毒实质上是指编制或在计算机程序中插入破坏计算机功能的数据，影响计算机使用并能自我复制的一组计算机指令或程序代码。一般病毒具有以下特性：可执行性——与其他合法程序一样，是一段可执行程序，但不是一个完整的程序，而是寄生在其他可执行程序上，当病毒运行时，便于合法程序争夺系统的控制权，往往会造成系统崩溃，导致计算机瘫痪。传染性——他通过各种渠道（磁盘、共享目录、邮件等）从已被感染的计算机扩散到其他机器上，在某种情况下导致计算机工作失常。潜伏性——一些编制精巧的病毒程序，进入系统之后不马上发作，隐藏在合法文件中，对其他系统进行秘密感染，一旦时机成熟，就四处繁殖、扩散。有的则执行格式化磁盘、删除磁盘文件、对数据文件进行加密等使系统死锁的操作。可触发性——病毒具有预定的触发条件，可能是时间、日期、文件类型或某些特定数据等。一旦满足触发感染的条件，它就会开始破坏工作，使病毒进行感染或攻击；如不满足，就会继续潜伏。针对性——有些病毒针对特定的操作系统或特定的计算机。隐蔽性——大部分病毒代码非常短小，也是为了隐蔽。一般都夹在正常程序之中，难以发现，一旦发作，则已经给计算机带来了不同程度的破坏 。

Virus definition （病毒）

电脑病毒的二元图。反病毒软件用此找寻和消灭病毒。

Worm （蠕虫）

可以在网络上繁殖的程序。蠕虫不能潜入其他应用程序。